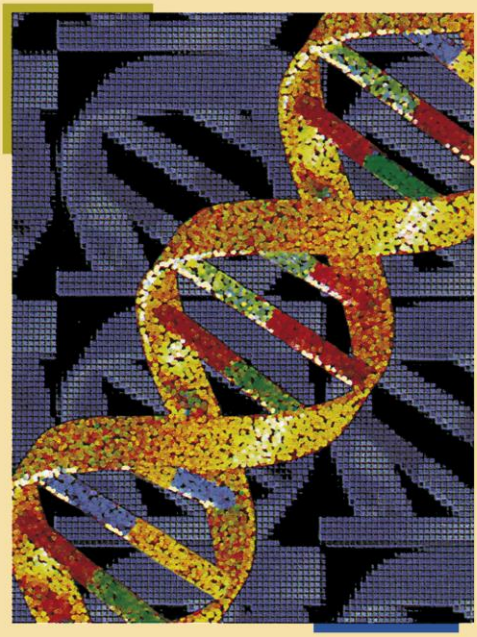
Revista de Derecho y Genoma Humano.

Genética, Biotecnología y Medicina Avanzada

Law and the Human Genome Review.

Genetics, Biotechnology and Advanced Medicine

Número Extraordinario 2019 / Extraordinary Number 2019



G.I. Cátedra de Derecho y Genoma Humano

Chair in Law and the Human Genome R.G.

Unión Europea
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Dykinson, S.L.

Gobierno de España
Ministerio de Ciencia, Innovación y Universidades

Revista de Derecho y Genoma Humano

Genética, Biotecnología y Medicina Avanzada

Law and the Human Genome Review

Genetics, Biotechnology and Advanced Medicine

Revista de Derecho y Genoma Humano

Genética, Biotecnología y Medicina Avanzada

Law and the Human Genome Review

Genetics, Biotechnology and Advanced Medicine

Número Extraordinario 2019 "Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas"

(Proyecto Ref.: DER2015-68212-R, financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional -FEDER-)

G.I. Cátedra de Derecho y Genoma Humano

Chair in Law and the Human Genome R.G.

2019
Universidad del País Vasco / Euskal Herriko Unibertsitatea

Editorial:
Dykinson, S.L.

Asistencia Editorial / Editorial Assistance:
G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU

Tfno.: +34 94 601 71 05 / +34 94 601 71 39
Email: derechoygenoma@bioderecho.eu

Página web: www.catedraderechoygenomahumano.es / www.bioderecho.eu

Distribución / Distribution:
- G.I. Cátedra de Derecho y Genoma Humano Universidad del País Vasco UPV/EHU
- Editorial Dykinson

Todas las partes de esta Revista pueden ser reproducidas citando el nombre completo de la Revista, el volumen, año y páginas en que fueron publicadas, así como, en su caso, el título del trabajo y el nombre del autor.

Parts of this Review may be reproduced provided that the full name of the Review, volume, year, page number(s) and, where appropiate, the title of the work and the name of the autor are quoted.

Descripción de la Revista: se trata de una revista en la que se reflexiona sobre las cuestiones jurídicas que plantea la genética humana desde el punto de vista del Derecho y también desde otras disciplinas.

Description of the Review: this is a re- view in which there are reflections on legal issues posed by human genetics from a legal point of view, as well as from other disciplines.

Esta Revista publica sus contenidos siguiendo la política de Acceso Abierto. Disponible en: www.dykinson.com/revistas/

This Review publishes its contents according to Open-Access Policy. Available at:
www.dykinson.com/revistas/

Publicación Semestral / Biannual Publication

Revista indexada en: SCOPUS, MEDLINE [PubMed], IN-RECJ, RESH, MIAR, LATINDEX, ISOC, DIALNET, DICE, SJR/ SCIMAGO, SHERPA/RoMEO, DULCINEA.

© G.I. Cátedra de Derecho y Genoma Humano
Universidad del País Vasco UPV/EHU

ISSN: 1134 - 7198
Depósito Legal: BI - 2670-94

Fotocomposición: Dykinson, S.L.

Consejo asesor / Comité de redacción
Advisory Board / Editorial Committee

Editor / Publisher
G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU, Bilbao. España.

Director / Editor

Romeo Casabona, Carlos M.	Director de G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU, Bilbao. España. Catedrático de Derecho Penal, Universidad del País Vasco UPV/EHU, Leioa. España.

Consejo asesor / Advisory Board

Alonso Bedate, Carlos	Investigador del Consejo Superior de Investigaciones Científicas, Centro de Biología Molecular, Universidad Autónoma de Madrid, Madrid. España.
Annas, George J.	Professor and Chair, Health Law Department, Boston University School of Public Health. Cofounder, Global Lawyers & Physicians (GLP), Boston, Massachusetts. USA.
Ayala, Francisco J.	Former President of the American Association for the Advancement of Science. Professor of Biological Sciences (Genetics and Evolution) and Professor of Philosophy. University of California, Irvine, California. USA.
Bergel, Salvador Darío	Titular de la Cátedra Unesco de Bioética. Facultad de Derecho. Universidad de Buenos Aires, Buenos Aires. Argentina.
Brena Sesma, Ingrid	Investigadora y Coordinadora del Núcleo de Estudios en Derecho y Salud del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. México.
Capron, Alexander Morgan	Professor of Law and Medicine. Co-Director of the Pacific Center for Health Policy and Ethics, University of Southern
Chadwick, Ruth	Director of CESAGen. Distinguished Research Professor. Cardiff University. South Wales. United Kingdom.
De Ángel Yágüez, Ricardo	Catedrático Emérito de Derecho Civil, Universidad de Deusto, Bilbao. España.
De Castro, Leonardo D. Eser, Albin	Professor of Philosophy, University of the Philippines. Philippines.
	Former Director, Max-Planck Institute of Foreign and Inter-
Gracia Guillén, Diego	Profesor Emérito de Historia de la Medicina y Director del Máster de Bioética, Universidad Complutense, Madrid.
Harris, John	Visiting Professor in Bioethics, Department of Global Health & Social Medicine, King's College London, London. United Kingdom. Former Professor of Bioethics and Aplied Philosophy. Universi- ty of Manchester. United Kingdom.
Knoepffler, Nikolaus	Professor Dr. mult. Professor of Applied Ethics. Director of the Cen- ter for Ethics, University Friedrich Schiller of Jena.
Lacadena, Juan-Ramón	Profesor Emérito de Genética, Universidad Complutense, Madrid. España.
Lenoir, Noelle	Former Delegate Minister, Paris, France.
Mayor Zaragoza, Federico	Former-Director General de la UNESCO, París. Francia.
Mazzoni, Cosimo Marco	Chair in Civil Law. University of Siena, Fiesole. Italy.
Macer, Darryl	President of the American University of Sovereign Nations, Arizona. USA.
McGee, Glenn	Professor and Director, Center for Medical Ethics Re- search, Albany Medical Center. Albany, USA.
Nys, Herman	Professor of Medical Law, University of Leuven, Leuven.
Roca Trías, Encarna	Belgium. Magistrada del Tribunal Constitucional, Madrid.

Smith, Hamilton O.	1978 Nobel Laureate in Medicine. Professor, Faculty of Medicine, Johns Hopkins University, Maryland. USA.
Soutullo, Daniel	Catedrático de Biología. IES Monte da Vila. O Grove, Pontevedra. España.

Comité de redacción / Editorial Committee

Armaza Armaza, Emilio José	Doctor en Derecho. Profesor de Derecho Penal e Investigador "Ramón y Cajal" de la Facultad de Derecho de la Universidad de Deusto, Bilbao. España.
Atienza Macías, Elena	Doctora en Derecho. Investigadora Postdoctoral "Juan de la Cierva". Universidad del País Vasco UPV/EHU, Leioa. España.
Casonato, Carlo	Full Professor of Comparative Constitutional Law, School of Law, Trento University, Trento. Italy. Member of the Italian Bioethics Committee, Rome. Italy.
Chueca, Ricardo	Catedrático de Derecho Constitucional de la Universidad de La Rioja, La Rioja. España.
Conal Fuertes, Iker	Licenciado en Derecho. Investigador Predoctoral del G.I. Cátedra de Derecho y Genoma Humano. Universidad del País Vasco UPV/EHU. Leioa. España.
De Miguel Beriain, Iñigo	Doctor en Derecho y en Filosofía. IKERBASQUE, Basque Foundation for Science. Universidad del País Vasco UPV/EHU, Leioa. España.
Duardo Sánchez, Aliuska	Doctora en Derecho. Investigadora Postdoctoral de la Universidad del País Vasco UPV/EHU, Leioa. España.
González de Cancino, Emilssen	Directora del Centro de estudios sobre Genética y Derecho en la Universidad Externado de Colombia, Bogotá. Colombia.
Grisolía, Santiago	Secretario Vitalicio de la Fundación Valenciana de Estudios Avanzados, Valencia. España.
Lazcoz Moratinos, Guillermo	Licenciado en Derecho. Investigador Predoctoral (FPU) del Ministerio de Educación y Formación Profesional. Universidad del País Vasco UPV/EHU. Leioa. España.
Mendizábal Allende, Rafael de Nicolás Jiménez, Pilar	Magistrado Emérito del Tribunal Constitucional, Madrid. España. Doctora en Derecho. Investigadora Permanente de la Universidad del País Vasco UPV/EHU, Leioa. España.
Pardo García, Juan Bautista	Ex-Presidente del Tribunal Superior de Justicia de la CAPV, Vitoria. España.
Payán Ellacuria, Ekain	Licenciado en Derecho. Investigador Predoctoral (FPI) de la Universidad del País Vasco UPV/EHU. Leioa. España.
Perin, Andrea	Doctor en Derecho. Profesor de Derecho Penal y Bioética, Facultad de Derecho, Universidad Andrés Bello, Chile.
Romeo Casabona, Carlos M.	Director de G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU, Bilbao. España. Catedrático de Derecho Penal de la Universidad del País Vasco UPV/EHU, Leioa. España.
Romeo Malanda, Sergio	Profesor Titular de Derecho Penal, Universidad de las Palmas de Gran Canaria, Las Palmas de Gran Canaria. España. Adjunct Associate Professor, Faculty of Law, Uni- versity of Tasmania, Australia.
Sartea, Claudio	Profesor de Filosofía del Derecho, Bioética, Teoría y Práctica de Derechos Humanos de la Facultad de Derecho de la Università degli Studi di Roma "Tor Vergata", Roma. Italia.
Simon, Jürgen	Professor of Economic Law and Private Environmental Law. Head of the Research Centre on Biotechnology & Law. University of Lüneburg, Lüneburg. F.R. Germany.
Urruela Mora, Asier	Doctor en Derecho y en Medicina. Profesor Titular de Derecho Penal de la Facultad de Derecho de la Universidad de Zaragoza, Zaragoza. España.

Comité Científico o Evaluadores Externos / Peer-Reviewers*

Abellán, Fernando	Abogado, Director de Derecho Sanitario Asesores. Doctor por la Universidad Complutense de Madrid en Medicina legal y forense. Profesor Asociado de la Escuela Nacional de Sanidad. Madrid. España.
Agovic, Amina	Post-doctoral researcher, Malmó University. Malmó. Sweden.
Alfonso Farnós, Iciar	Médico especialista en Farmacología Clínica. Farmacóloga y Secretaria del Comité Ético de Investigación Clínica de Euskadi (CEIC-E). Vitoria. España.
Alkorta Idiakez, Itziar	Profesora Titular de Derecho Civil de la Universidad del País Vasco UPV/EHU. San Sebastián. España.
Andorno, Roberto	Investigador de la Facultad de Derecho de la Universidad de Zúrich. Zúrich. Suiza.
Armaza Galdos, Julio	Catedrático de Derecho Penal de las Universidades Católica de Santa María y Nacional de San Agustín. Arequipa. Perú.
Bellver Capella, Vicente	Catedrático Acreditado de Filosofía del Derecho de la Universidad de Valencia. Valencia. España. Miembro del Comité de Bioética de España.
Benítez Ortúzar, Ignacio F.	Catedrático de Derecho Penal. Director del Departamento de Derecho Penal, Filosofía del Derecho, Filosofía Moral y Filosofía de la Universidad de Jaén. Jaén. España.
Brena Sesma, Ingrid	Investigadora y Coordinadora del Núcleo de Estudios en Derecho y Salud del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. México.
Corti Varela, Justo	Investigador Post-Doctoral del Instituto de Estudios Europeos. Profesor de Derecho del área UE y Relaciones Internacionales de la Facultad de Derecho de la Universidad CEU-San Pablo. Madrid. España.
De la Cuesta Arzamendi, José Luis	Catedrático de Derecho Penal. Presidente de la Asociación Internacional de Derecho Penal (AIDP-IAPL). Director del Instituto Vasco de Criminología de la Universidad del País Vasco UPV/EHU. San Sebastián. España.
De Montalvo Jääskeläinen, Federico	Profesor Propio Adjunto de Derecho Constitucional de la Facultad de Derecho (ICADE), Universidad Pontificia Comillas. Madrid. España. Presidente del Comité de Bioética de España.
Douglas, Conor M.W.	Post-Doctoral Researcher Community Genetics EMGO Institute for Health and Care Research. VU University Medical Center. Amsterdam. The Netherlands.
Ducato, Rossana	Postdoctoral Researcher. Ph.D. in Comparative and European Legal Studies, Institut pour la recherche interdisciplinaire en sciences juridiques. Leuven, Belgium.

* Listado elaborado a partir de las evaluaciones realizadas desde el Número 32 Enero-Junio de 2010 hasta la fecha de cierre de esta edición. Se ha contado con el consentimiento expreso de los evaluadores para aparecer en este listado. Algunos evaluadores han declinado aparecer en este listado.

List of external reviewers panel compiled from evaluations made starting from the Review Number 32 January - June 2010 until the closing date of this issue. The Advisory Board has received the evaluators' consent to appear at this panel. Some reviewers have declined this proposal.

Etxeberria Guridi, José Francisco	Catedrático de Derecho Procesal de la Universidad del País Vasco UPV/EHU. San Sebastián. España.
Femenía López, Pedro J.	Catedrático de Derecho Civil de la Universidad de Alicante. Alicante. España.
Freire de Sá, Maria de Fátima	Magister en Derecho por la Pontificia Universidad Católica de Minas Gerais (PUC Minas) y Doctora en Derecho Constitucional por la Universidad Federal de Minas Gerais (UFMG). Investigadora del Centro de Estudios en Bioderecho - CEBID. Belo Horizonte. Brasil.
García Amez, Javier	Doctor en Derecho. Grupo Gestión de la F.A., Hospital Vital Álvarez Buylla. Servicio de Salud del Principado de Asturias. Oviedo. Asturias.
Libano Beristain, Arantza	Profesora Agregada de Derecho Procesal de la Universidad Autónoma de Barcelona. Barcelona. España.
Martín Uranga, Amelia	Secretaria de la Plataforma Tecnológica Española Medicamentos Innovadores, Farmaindustria. Madrid. España.
Moya Simarro, Andrés	Catedrático de Genética de la Universidad de Valencia. Director Científico del Centro Superior de Investigación en Salud Pública de Valencia. Presidente de la Sociedad Española de Biología Evolutiva. Valencia. España.
Myszczuk, Ana Paula	Doctor of Economic and Socialenvironmental Law, PUCPR. Associate Professor at Federal University of Technology of Paraná. Curitiba, Brazil.
Nicol, Dianne	Professor of Law, Chair of Academic Senate. University of Tasmania. Tasmania. Australia.
Orfao de Matos, Alberto	Catedrático del Departamento de Medicina de la Universidad de Salamanca. Investigador Principal de grupo del Centro de Investigación del Cáncer. Director Científico del Banco Nacional de ADN. Salamanca. España.
Penasa, Simone	Research Assistant in Comparative Constitutional Law. Faculty of Law, University of Trento. Trento. Italy.
Pérez Álvarez, Salvador	Profesor Titular de Universidad. Facultad de Derecho. Coordinador de la Zona Norte del Centro Asociado a la UNED de Madrid, Universidad Nacional de Educación a Distancia (UNED). Madrid. España.
Plomer, Aurora	Professor of Law and Bioethics. University of Sheffield. Sheffield. United Kingdom.
PreuB, Dirk	Research assistant at the Center for Ethics. University Friedrich Schiller of Jena. Jena. Germany.
Ramiro Avilés, Miguel A.	Profesor Titular de Filosofía del Derecho de la Universidad de Alcalá. Madrid. España.
Rey del Castillo, Javier	Secretario de la Comisión Nacional de Reproducción Humana Asistida. Madrid. España.
Robienski, Jürgen	Lawyer in Hannover and Müden / Aller. Research associate at Hannover Medical School (MHH) and the Center for eth- ics and law in the life sciences. Hannover. Germany.
Rodríguez López, Raquel	Facultativo de Genética Molecular, Unidad de Genética, Hospital Infanta Cristina. Servicio Extremeño de Salud. Consejería de Sanidad y Dependencia de la Junta de Extremadura. Badajoz. España.
Sandor, Judit	Professor. Director of the Center for Ethics and Law in Bi- omedicine (CELAB). Budapest. Hungary.
Schneider, Ingrid	Senior Researcher, FSP BIOGUM, Centre for Biotechnolo- gy, Society and the Environment - Medicine, and University Lecturer, Department of Political Science, University of Hamburg. Hamburg, Germany.

Seoane, José Antonio	Profesor Titular de Filosofía del Derecho de la Universidad de La Coruña. La Coruña. España. Profesor de Filosofía del Derecho de la Universidad de Lleida.
Silveira Gorski, Héctor Claudio	Director Adjunto del Observatorio del Sistema Penal y los Derechos Humanos de la Universidad de Barcelona. Barcelona. España.
Tejada Mínguez, Mª Isabel	Responsable del Laboratorio de Genética molecular, Servicio de Genética del Hospital Universitario Cruces. Barakaldo. España.
Ter Meulen, Ruud	Chair, Director Centre for Ethics in Medicine School of Social and Community Medicine Faculty of Medicine and Dentistry University of Bristol. Bristol. United Kingdom.

Revista de Derecho y Genoma Humano

Genética, Biotecnología y Medicina Avanzada

Law and the Human Genome Review

Genetics, Biotechnology and Advanced Medicine

Número Extraordinario 2019 "Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas"

Sumario / Summary

Opinión / Opinion

Documento de información sobre la utilización de los datos de la historia clínica con fines de investigación biomédica en contextos de bigdata
Nuria Terribas I Sala (Coordinadora)
Miembros Del Proyecto De Investigación Bigdatius (Bilbao, España) 17

Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI (En cumplimiento del Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)
Iciar Alfonso Farnós / Guillermo Alcalde Bezhold (Vitoria, España)
Míriam Méndez García (Barcelona, España) 25

Doctrina / Articles

Nuevos desafíos en torno al big data
Gustavo Merino Gómez (Santander, España) 37

Utilización de tecnología Big Data en investigación clínica
Guillermo Alcalde Bezhold / Iciar Alfonso Farnós (Vitoria, España) 55

Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud
Carlos María Romeo Casabona (Bilbao, España) 85

Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos
Pilar Nicolás Jiménez (Bilbao, España) 129

Implicaciones jurídicas de la internacionalización de la tecnología del big data y derecho internacional privado
Alfonso Ortega Giménez (Alicante, España) 169

La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018
Míriam Méndez García (Barcelona, España)
Iciar Alfonso Farnós (Vitoria, España) 205

Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo
Inmaculada Vivas Tesón (Sevilla, España) 233

Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Big data
Itziar Alkorta Idiakez (San Sebastián, España) 273

Pruebas genéticas en los tratamientos de reproducción asistida, con especial referencia a los tests de portadores y matching genético. Controversias en materia de información
Fernando Abellán-García Sánchez (Madrid, España) 325

Evaluación de proyectos de investigación con tecnología Big Data por un Comité de Ética de la investigación
Iciar Alfonso Farnós / Guillermo Alcalde Bezhold (Vitoria, España)
Míriam Méndez García (Barcelona, España) 349

Protección de los datos personales de salud en el proceso penal: efectos en la valoración de la prueba
Miren Josune Pérez Estrada (Bilbao, España) 395

Transferencias internacionales de datos genéticos y datos de salud con fines de investigación
Mikel Recuero Linares (Bilbao, España) 413

Informes / Reports

El derecho de los pacientes a sus copyrights
Virginia Díaz Gorriti / Rosa Mª Añel Rodríguez (Bilbao, España) 437

IntimidAPP: Los problemas del tratamiento de datos biosanitarios en wearables y apps para móviles
Alberto Hidalgo Cerezo (Madrid, España) 449

Participative consent: Beyond broad and dynamic consent for health big data resources
María Villalobos-Quesada (Barcelona, Spain) 485

La asistencia sanitaria transfronteriza a la luz del Reglamento General de Protección de Datos
Daniel Jove Villares (A Coruña, España) 511

Tratamiento seguro de datos como factor de integración europea: implicaciones legales en el ámbito de la salud pública en Georgia
David Ruano Delgado (Bayona, Francia)
Nikoloz Phiphia (Tiflis, Georgia) 525

Una aproximación al big data y al blockchain sanitario y su implicación en la protección de datos personales
Lorena Pérez Campillo (Madrid, España) 547

Análisis doctrinal y jurisprudencial de los delitos de descubrimiento y revelación de secretos en el ámbito sanitario
Iker Conal Fuertes (Bilbao, España) 569

Documentos / Documents

Informe 073667/2018 de la Agencia Española de Protección de Datos sobre la incidencia en el ámbito de la investigación biomédica del Reglamento General de Protección de Datos 601

The European Data Protection Board Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b) 611

Bibliografía / Bibliography

Recensiones de libros y revistas / Books and journals reviews

La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud
Lucía Cristea Uivaru
(Elena Atienza Macías) 623

Referencias bibliográficas y documentales / References to books, articles in periodicals and to other documents 629

OPINIÓN / OPINION

Documento de información sobre la utilización de los datos de la historia clínica con fines de investigación biomédica en contextos de *bigdata*[*]

Information sheet on the use of clinical record for biomedical research purposes in bigdata contexts

AA.VV.[**]

DOI: 10.14679/1130

1. Justificación del documento

Uno de los objetivos del proyecto Bigdatius es proponer herramientas útiles para la adecuada gestión masiva de datos con fines de la investigación biomédica, de manera que se potencie la utilidad de la información clínica en beneficio del avance de la ciencia, siempre garantizando los derechos del paciente como eje del tratamiento de los datos. Este documento es una propuesta sobre los contenidos esenciales que el paciente debe conocer si se

* Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos –*Big Data*–. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.:DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

** La redacción de este documento ha sido coordinada por Núria Terribas i Sala en el marco del mencionado proyecto de investigación BIGDATIUS. En la redacción han participado: Alcalde Bezhold, Guillermo / Alfonso Farnós, Iciar / Alkorta Idiakez, Itziar / Atienza Macías, Elena / Bilbao Urquiola, Roberto / De Miguel Beriain, Iñigo / Emaldi Cirión, Aitziber / Méndez García, Miriam / Nicolás Jiménez, Pilar / Puente, Mercedes / Romeo Casabona, Carlos / Vivas Tesón, Inmaculada.

van a utilizar sus datos clínicos en este contexto. Está basado en las exigencias normativas en los títulos que legitiman el tratamiento de los datos, más allá del consentimiento del titular.

Se trata de un modelo que podría utilizarse en diferentes sistemas de tratamiento de los datos, gestionados por autoridades sanitarias, hospitales o centros de investigación. Por esta razón algunos puntos se han dejado abiertos, sin concretar una descripción del escenario en que se desenvuelve el tratamiento, pero sí indicando que, en su caso, se debería incluir.

2. Presentación del documento

El uso de datos sanitarios agregados de los ciudadanos usuarios de nuestro sistema de salud, con fines de investigación biomédica, va adquiriendo cada vez mayor importancia y puede suponer una **ayuda inestimable a la investigación revirtiendo en beneficio de toda la comunidad.** El sistema de salud trabaja para dar la mejor atención a las personas y a su vez dirige su actuación a la mejora de la salud de la ciudadanía a partir de los principios de la medicina personalizada, basada en la evidencia científica. En este contexto, el acceso a información de calidad es un factor clave para seguir creciendo en investigación e innovación y dotarse de herramientas para la mejora de la asistencia. Uno de los mecanismos imprescindibles para alcanzar esos objetivos es poder compartir la información almacenada de la que disponemos en el sistema.

Así, la información de que disponemos en las historias clínicas de los pacientes incluye una gran cantidad de datos útiles para los investigadores que intentan conocer más sobre muchas enfermedades hoy incurables o para mejorar el tratamiento de otras más recurrentes y que afectan a un grupo muy amplio de población (enfermedades cardiovasculares, cáncer, demencias, etc). **Combinando información procedente de registros clínicos masivos, los investigadores pueden obtener conocimientos de gran valor puesto que los resultados son más sólidos basados en una población mayor y no de grupo reducido**.

Los datos de salud que constan en la historia clínica forman parte de esa gran cantidad de información que puede tener un **uso secundario importante para investigación a gran escala, más allá del uso prioritario y principal como es la asistencia y atención a los problemas de salud** de los pacientes.

Es imprescindible que este uso secundario de los datos clínicos se lleve a cabo siempre respetando las normas éticas de buenas prácticas en investigación y la legislación vigente. **El respeto a los derechos de los ciudadanos es prioritario**.

Los **principios éticos** que sustentan la investigación con datos clínico-asistenciales de los ciudadanos:

- **Respeto** a las personas: todo ciudadano que colabore dando acceso a sus datos para investigación debe hacerlo con la información necesaria y con garantías de respeto a la confidencialidad mediante la protección de los datos y evitando su uso indebido.

- **Solidaridad**: la autorización para el uso secundario de los datos de salud para investigación se fundamenta en la solidaridad de la ciudadanía con el sistema sanitario de salud y como forma de retorno a la comunidad mediante la aportación de nuevo conocimiento.

- **Justicia**: el uso de datos para investigación priorizará siempre aquellos proyectos que pretendan resolver problemas relevantes de salud, en especial en poblaciones vulnerables.

- **Responsabilidad**: el uso de información de los ciudadanos siempre deberá hacerse cumpliendo las buenas prácticas en investigación, evitando cualquier perjuicio y garantizando un buen uso que revierta en la comunidad. De igual modo, el uso de datos se regirá siempre por un criterio de minimización de modo que se utilizarán siempre los mínimos indispensables para la obtención del resultado previsto en la investigación de que se tratase, y no más allá de estos.

El Reglamento (UE) 2016/679 General de Protección de Datos y la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de los Derechos Digitales, son el **nuevo marco normativo regulador de esta materia. La interpretación de esta nueva legislación reviste ciertas dificultades,** pero se puede afirmar con rotundidad que el principio de responsabilidad en el tratamiento de los datos, que supone implementar garantías adecuadas para los derechos de los sujetos y el principio de transparencia, se constituyen en dos de sus pilares fundamentales: **la información sobre la forma en que los datos se van a gestionar es la principal garantía que tienen los ciudadanos en relación con el control de sus datos.**

Este documento se ha elaborado con el objetivo **de orientar sobre el contenido de la información a facilitar a las personas para realizar estudios con tecnología bigdata,** de acuerdo con los principios éticos y con la normativa vigente. Está enfocado a la utilización de datos en entornos tecnológicamente avanzados y de intercambio de información. Por esta razón, **no se incluye la posibilidad de tratamiento de datos con identificadores de personas**, cuyo almacenamiento, utilización y cesión con fines de investigación biomédica a través de tecnologías de bigdata podría resultar muy difícil de adaptar a los procedimientos establecidos por la normativa para esta categoría de datos y exigiría otros requerimientos.

3. Información sobre utilización de los datos de la historia clínica con fines de investigación biomédica

Finalidad de la Investigación

La finalidad de la investigación biomédica es mejorar el conocimiento de las enfermedades y su posible tratamiento en beneficio de toda la comunidad. El estudio de la información almacenada en las historias clínicas y su correlación con otros registros de datos es muy útil para alcanzar estos objetivos. Con este propósito, sus datos clínicos podrán ser utilizados en proyectos de interés científico y evaluados por un comité de ética, a través de procedimientos que garanticen el respeto de todos sus derechos.

Protección de datos y confidencialidad

(Describir el sistema de almacenamiento de los datos: en historia clínica o en otro repositorio donde se vuelque la información clínica).

Los datos, según la naturaleza del estudio y sus objetivos, podrán ser utilizados en una de estas dos modalidades:

a) Como datos ANONIMIZADOS: desvinculando totalmente de los datos cualquier información directa o indirectamente identificativa, de manera que ya no sea posible relacionarlos con una persona determinada.

b) Como datos SEUDONIMIZADOS: desvinculando de los datos cualquier información directamente identificativa, de manera que los investigadores no podrán relacionarlos con una persona determinada,

Los datos de identificación personal serán sustituidos por un código, que los investigadores no podrán descifrar. Además, se comprometerán a no identificarle por ningún medio. La clave para vincular de nuevo los datos con una persona determinada estará únicamente a disposición del centro donde se obtuvieron los datos clínicos.

Sea cual fuera la modalidad de uso de los datos, en función del tipo de proyecto y sus objetivos, todo profesional implicado en el manejo de los mismos se debe a la obligación de secreto profesional que le vincula en toda su actividad.

El tratamiento de los datos con fines de investigación biomédica se prolongará durante el tiempo necesario en relación con los objetivos que lo justifican, y no se prolongará con otros propósitos.

Especificidad de los datos genéticos

Por su especial sensibilidad, la utilización de datos genéticos, incluso anonimizados, con fines de investigación biomédica, se llevará a cabo con garantías reforzadas, que se adaptarán a las circunstancias concretas de cada investigación y serán evaluadas específicamente por un Comité de Ética de la Investigación.

Responsable del repositorio de datos y ejercicio de derechos

Los datos de la historia clínica que podrán ser utilizados para investigación quedarán bajo la responsabilidad y control del responsable del tratamiento establecido al efecto (añadir los datos del resposable).

Los derechos de acceso, rectificación, limitación, oposición y supresión recogidos en la Ley 3/2018 de Protección de Datos Personales así como el Reglamento (UE) 2016/679, se podrán ejercer ante el Delegado de Protección de Datos –DPO– (Datos de contacto ……..).

Aún así, y de conformidad con la legislación vigente, el ejercicio del derecho de supresión no será posible en el supuesto de que los datos hayan sido anonimizados, así como tampoco respecto a los seudonimizados en cuanto al uso que ya se hubiese hecho de ellos con anterioridad al ejercicio del derecho.

Por otra parte, usted puede dirigirse a la Agencia de Protección de Datos para presentar reclamaciones relacionadas con el tratamiento de sus datos.

Supervisión ética

El uso de datos para investigación deberá ser autorizado por el responsable del fichero en el que se recogen los datos de todas las historias clínicas, si bien previa revisión de la petición (proyecto de investigación, finalidades, característica de las muestras de datos, etc.) por parte de un Comitè de Ética de la investigación específico que validará cada proyecto, velando para que los estudios sigan las más estrictas normas éticas y legales, y ponderando la idoneidad de los datos solicitados, así como la necesidad de que se mantengan seudonimizados si así se requiere.

Carácter altruista de la cesión de datos

La cesión de los datos clínico asistenciales de las historias clínicas para su uso en investigación es gratuita. Ello supone que el titular de esos datos no tendrá derechos sobre posibles beneficios comerciales de los descubrimientos que puedan conseguirse como resultado de la investigación biomédica. La razón que legitima esta gratuidad es la solidaridad, ya que todos nos beneficiamos de los resultados de la investigación, facilitada por la colaboración de pacientes y usuarios, y el bien a proteger en última instancia es el bien común.

Información sobre los resultados de la investigación

Se proporcionará información sobre los proyectos de investigación en que se hayan utilizado los datos, así como sobre sus resultados si el sujeto así lo solicita y si es posible trazar su origen, (Indicar dónde se tiene que dirigir para solicitarla o si se ~~se~~ puede acceder directamente a través de alguna plataforma).

Si de la utilización de datos seudonimizados se obtuviera información relevante que pudiera afectar a la salud del titular o a la de su familia, se habilitarán los medios oportunos para contactar y ofrecer la posibilidad de conocer dicha información, así como para aconsejar la conveniencia de transmitir esta información a sus familiares en caso necesario. A efectos de un eventual contacto se utilizarán los datos que figuren en el historial clínico. No obstante, se respetará el derecho a decidir que no se le comunique ningún resultado.

Rechazo a la utilización de los datos para investigación

Si la persona titular de los datos clínicos no desea que estos sean utilizados para la investigación biomédica, no se utilizarán ni se incluirán en los registros agregados a tal efecto. Para ello, deberá manifestarlo de forma explícita a su médico o al personal responsable del tratamiento de datos en el centro sanitario donde la persona sea atendida habitualmente.

Ese rechazo en ningún caso repercutirá negativamente en el cuidado asistencial que la persona deba recibir del sistema sanitario.

El personal sanitario responsable que le ha comunicado esta información está a su disposición para aclarar cualquier duda que pueda tener, ahora o en el futuro, en relación con ello.

Agradecemos su solidaria colaboración.

Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI

(En cumplimiento del Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)*

Questionnaire/guide for the evaluation of research projects with personal data by a Research Ethics Committee

(In compliance with European Regulation 2016/679 on data protection and Fundamental Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights)

Iciar Alfonso Farnós

Comité de Ética de la Investigación con medicamentos de Euskadi (Vitoria, España)

Guillermo Alcalde Bezhold

Comité de Ética de la Investigación Hospital Universitario Araba (Vitoria, España)

Miriam Méndez García

Comité de Ética de la Investigación con medicamentos Hospital Clinic (Barcelona, España).

DOI: 10.14679/1131

---

* Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos –*Big Data*–. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.:DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

1. Aspectos generales a revisar en cada centro

- Que se ha analizado si es necesario realizar una evaluación de impacto en la Protección de Datos Personales (EIPD).
- Que el responsable del tratamiento esté adherido a algún código de conducta o mecanismo de certificación que garantice un nivel de seguridad adecuado al riesgo.
- Que cuente, si es preciso, con el asesoramiento de un delegado de protección de datos.

2. Aspectos que debe revisar un CEI en cada proyecto

		Si No No procede
Protocolo/ memoria científica	• Descripción de la justificación científica y objetivos del estudio; definición de las variables de resultado y del análisis estadístico previsto. • Descripción del tratamiento que va a aplicarse a los datos obtenidos, valoración de los riesgos potenciales para la privacidad y qué medidas van a adoptarse para reducirlos, aplicando el principio de minimización de datos (adecuados, pertinentes y limitados a lo necesario en relación a los fines de la investigación).	° ° ° ° ° °

Idoneidad del Investigador/ Responsable del tratamiento	• Se han aportado los documentos que acreditan su formación y experiencia en investigación.
	• Se ha aportado el compromiso escrito referente a:
	  • Utilizar los datos sólo para los fines previstos;
	  • Garantizar la confidencialidad de la información y no realizar ninguna actividad de reidentificación de los participantes, ni ceder los datos a terceros no autorizados;
	  • Cumplir las exigencias legales y del comité respecto al seguimiento, informando periódicamente sobre la marcha del estudio.
	• Si se van a tratar los datos seudonimizados se ha aportado un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
	• Se ha aportado la información sobre el encargado del tratamiento de los datos, cuando no coincida con el responsable del tratamiento, en relación a conocimientos especializados, fiabilidad y recursos.
	• Se ha firmado un contrato con el encargado del tratamiento.
		° ° °
		° ° °
		° ° °
		° ° °
		° ° °

		Si No No procede
Idoneidad de los medios previstos para el tratamiento de los datos	• Se ha informado sobre las medidas de seguridad para garantizar la privacidad. • Se aporta la información sobre el servidor en el que se van a alojar los datos y las medidas de seguridad que van a adoptarse: a) Se utilizan servidores que cumplen con un plan de gestión de protección de datos, como por ejemplo las bases de datos alojadas en el servidor del centro sanitario/institución/servicio de salud cuando se ha realizado una EIPD. b) Si no se dispone de un plan de gestión de protección de datos se describen las medidas de seguridad adicionales, tanto en el protocolo, como en el contrato con el encargado del tratamiento: • Cuadernos de recogida de datos electrónicos (CRFe) ubicados en la web del promotor. • Datos seudonimizados alojados en nubes (Google drive, dropbox, etc ...): las plataformas estarán ubicadas en Europa o adscritas al Privacy Shield: https://www.privacyshield.gov/list. • Se describen las medidas de seguridad de otros medios: software,…	° ° ° ° ° ° ° ° ° ° ° ° ° ° °

3. Aspectos que debe revisar un CEI en cada proyecto

		SI No No procede
Evaluación de las medidas de seguridad previstas en el tratamiento de los datos	• Se informa sobre cómo se accede a los datos. • Se aporta el formulario de recogida de datos/base de datos, en los que se comrpueba que no se plantea recoger datos identificativos. • Si los datos se recogen codificados se informa sobre quién custodia el código que permitiría la identificación del titular de los datos. • Se aplican los procesos de anonimización y/o seudonimización. • Si se tratan los datos seudonimizados se informa sobre quién y como se va a realizar la seudonimización y de las medidas de seguridad específicas que van a adoptarse para evitar la reidentificación y el acceso de terceros no autorizados.	° ° ° ° ° ° ° ° ° ° ° ° ° ° °
Garantía de transparencia	• Se adjunta un compromiso de publicación de resultados.	

		SI No No procede
Transferencia de datos fuera del centro	• Si los datos van fuera del centro se ha aportado un contrato con el encargado de tratamiento. Ej: cuando se contratan empresas para gestionar desplazamientos de pacientes que están participando en un estudio de investigación y les ceden datos identificativos. • Si se contempla la transferencia internacional de datos fuera de la Unión Europea se ha adjuntado un acuerdo que garantice que el país o la entidad de destino cumplen con los requisitos mínimos que exige la normativa europea (p. ej. estar inscritos en el Privacy Shield).	° ° ° ° ° °
Revisión del consentimiento informado	• Cuando proceda solicitar el consentimiento informado, el documento incluye los diferentes apartados exigidos por el RGPD/LOPD-GDD (ver modelo anexo)	° ° °

4. Cuando se acepta la exención de consentimiento informado

		SI NO No procede
Situaciones en la que se puede aceptar la exención de consentimiento	• Cuando el interesado ha otorgado un consentimiento previo amplio, que incluya categorías relacionadas con la especialidad médica o investigadora para la que se dio el consentimiento inicial. El CEI debe verificar si el objetivo del estudio está enmarcado en los fines para los que se consintió. • Se plantea reutilizar datos obtenidos en un proyecto anterior, para el que se dio un consentimiento concreto, para un proyecto similar (de la misma línea o ámbito de investigación). El CEI debe revisar: o El objetivo del estudio: si el objetivo del proyecto a evaluar no está enmarcado en los objetivos para los que el titular de los datos consintió, debe solicitarse un nuevo consentimiento expreso para el proyecto. o Que la información del nuevo uso se publique en la página web corporativa del centro donde se realice la investigación o estudio clínico. o Que se notifique a los participantes la existencia de esta información por medios electrónicos o Que se establezcan mecanismos para posibilitar el rechazo a la utilización de los datos para investigación • Puede aceptarse la exención si el estudio se va a realizar con datos anonimizados o seudonimizados. En este caso el CEI debe comprobar que se dispone de las garantías adicionales establecidas por el RGPD y la LOPD-GDD.	° °

MODELO DE HOJA DE INFORMACIÓN AL PACIENTE PARA REALIZAR UN ESTUDIO CON DATOS PERSONALES

Muy Sr./Sra. nuestro:

Le proponemos participar en el estudio de investigación, de título ***"xxxx***", promovido por xx (si es un promotor externo), que va a ser realizado por xx como investigador principal. Siguiendo las guías éticas internacionales y la legislación vigente, este estudio ha sido aprobado por el comité de ética de la investigación del hospital/centro.

Antes de que usted decida si va a participar o no es importante que lea detenidamente la siguiente información, que realice todas las preguntas y solicite aclaración de todas las cuestiones que crea conveniente.

¿Tengo que participar?

La participación en el estudio es completamente voluntaria. Rechazarla no acarreará ningún deterioro en la calidad de la asistencia y el tratamiento de su enfermedad o proceso. Además, podrá retirarse en cualquier momento del estudio, sin tener que dar explicaciones y sin que ello repercuta en los cuidados médicos que recibe.

¿Objetivo del estudio?

Describir el fin y/o los fines y usos previstos de la recogida de datos personales para realizar el proyecto propuesto. Debería darse la opción de otorgar el consentimiento para determinadas áreas de investigación o partes de proyectos de investigación.

Información sobre los datos que se van a recoger

Información sobre quién va a tratar los datos; a quién los pueden ceder; quiénes son sus destinatarios o del plazo de conservación de los datos.

¿En qué consiste el estudio y cómo se va a llevar a cabo?

Debe describirse si la recogida de datos es puntual o si hay un seguimiento y la duración del mismo.

¿Qué beneficios puedo esperar por el hecho de participar en el estudio?

Explicar que en principio no se esperan beneficios. Informar, cuando corresponda, acerca de la posible generación de beneficios comerciales y/o propiedad intelectual.

¿Cómo van a ser tratados mis datos?

Sus datos personales serán registrados de forma estrictamente confidencial, conforme con el Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. En cumplimiento de esta legislación se le informa sobre el cumplimiento de las siguientes exigencias respecto al tratamiento de sus datos:

- **Identidad del responsable del tratamiento de los datos** y ante quién y cómo pueden ejercitar sus derechos (ante el investigador principal del estudio o el Delegado de Protección de Datos del centro).

- **Identidad del encargado del tratamiento de los datos.** Explicar quién va a tratar los datos personales.

- **Medidas de seguridad para proteger la privacidad y los riesgos para la confidencialidad.** Debe informarse sobre cómo se van a tratar los datos: anonimizados, seudonimizados o codificados, y durante cuanto tiempo se van a conservar los datos.

- Si se recogen los datos anonimizados debe informarse sobre el alcance real de los procesos de anonimización, que puede que no garanticen totalmente la irreversibilidad. Debe informarse sobre los posibles riesgos asociados a la reidentificación y la revelación de información confidencial.

- Deben explicarse las reglas de administración/gobernanza de la base de datos o formulario de recogida de datos; quién los gestiona, información sobre las medidas de seguridad del servidor en el que se van a almacenar los datos,…

- **Información sobre los derechos de los titulares de los datos**

- Se informa sobre el derecho de acceso, modificación, oposición y cancelación[1] de los datos que van a recogerse en este estudio; derecho a limitar el tratamiento de datos que sean incorrectos o inexactos, solicitar una copia o que se trasladen a un tercero (portabilidad) los datos que se facilitan para el estudio.

- Ejemplo de párrafo: Para ejercitar sus derechos, diríjase al investigador principal del estudio ***[*o al/a la **Delegado/a de Protección de Datos** del centro/institución en [dirección/link]*.] Además, podrá ampliar información en materia de protección de datos en la siguiente dirección web: xxx. Así mismo tiene derecho a dirigirse a la Agencia de Protección de Datos si no quedara satisfecho.

- Tanto el centro sanitario como el investigador son responsables respectivamente del tratamiento de sus datos y se comprometen a cumplir con la normativa de protección de datos en vigor. Los datos recogidos para el estudio estarán identificados mediante un código, de manera que no se incluya información que pueda identificarle, y sólo su médico del estudio/colaboradores podrá relacionar dichos datos con usted y con su historia clínica. Por lo tanto, su identidad no será revelada a ninguna otra persona salvo a las autoridades sanitarias, cuando así lo requieran o en casos de urgencia médica. Únicamente los comités de ética de la investigación y los representantes de la Autoridad Sanitaria en materia de inspección podrán acceder a su historia clínica para comprobar los datos personales, los procedimientos del estudio clínico y el cumplimiento de las normas de buena práctica clínica (siempre manteniendo la confidencialidad de la información).

- Usted tiene derecho a **retirar el consentimiento en cualquier momento** y la información identificable de la base de datos de salud o el formulario de recogida de datos, así como el derecho a solicitar y recibir información sobre sus datos y su uso.

Debe explicarse que si la información se anonimiza la persona no podrá saber qué se hace con su información, ni tampoco retirar su consentimiento.

En el caso de datos genéticos, debe informarse sobre los derechos amparados en la Ley 14/2007 de investigación biomédica.

---

[1] Con las salvaguardas legales respecto a los datos ya recogidos cuando sean pertinentes para los fines del estudio.

Debe informarse sobre la opción futura de reutilizar los datos en estudios en finalidades relacionadas. En este caso, la información de los estudios estará disponible en la página web del centro (xxx). Además debe solicitarse la dirección de correo electrónico para recibir la citada información.

¿Qué incomodidades o riesgos pueden suponer mi participación en el estudio?

Explicar los posibles riesgos para la confidencialidad, especialmente si los datos salen fuera del centro, describiendo los posibles riesgos asociados a la transferencia fuera de la Unión Europea, en su caso.

¿Mi participación me supondrá algún coste o compensación económica?

Explicar que la participación en el estudio no supondrá ningún coste económico, así como tampoco será recompensado económicamente por ello.

Si usted tiene alguna duda o quiere más información, no dude en consultar con el médico responsable que le está solicitando este consentimiento.

GRACIAS POR LEER ESTA INFORMACIÓN

5. Consentimiento informado para los participantes

Título del estudio: ***"xxx"***

Investigador principal xxx

Servicio de xxx. Hospital/centro xxxx

Yo, (nombre y apellidos) …… manifiesto que he sido informado/a del presente estudio y:

- He leído y entendido la hoja de información que se me ha entregado.
- He podido hacer preguntas sobre el estudio y sobre mis derechos.
- He recibido suficiente información sobre el estudio.
- Comprendo que mi participación es voluntaria.

- Comprendo que puedo retirarme del estudio:
  - Cuando quiera.
  - Sin tener que dar explicaciones.
  - Sin que esto repercuta en mis cuidados médicos.
- Comprendo que mi participación en el estudio no conlleva ningún perjuicio para mi salud.
- He sido informado/a de que mis datos personales serán protegidos, que los resultados de mi evaluación personal serán estrictamente confidenciales.

EN CONSECUENCIA DOY MI CONSENTIMIENTO PARA FORMAR PARTE DE ESTE PROYECTO DE INVESTIGACION.

…… ……..	
Firma del/la paciente	Firma del médico responsable
……..…….....	……..…….....
Nombre y apellidos	Nombre y apellidos
Fecha ……/……/20……	Fecha ……/……/20……

DOCTRINA / ARTICLES

Nuevos desafíos en torno al *big data*[*]

New challenges around big data

Gustavo Merino Gómez

Investigador del Grupo de investigación Derecho Sanitario y Bioética (GRIDES) de IDIVAL (Santander, España)

DOI: 10.14679/1132

Sumario / Summary: 1. Introducción y Marco normativo. 2. Avances tecnológicos y nuevos retos. 3. El consentimiento del sujeto como calve del sistema. 4. La seguridad de los datos como presupuesto básico. 5. Conclusiones. 6. Bibliografía.

Resumen / Abstract: Los nuevos reglamentos europeos sobre ensayos clínicos, dispositivos médicos y el nuevo Reglamento Europeo sobre protección de datos, incorporan varios preceptos para garantizar el derecho a la vida privada y la protección de datos en materia de salud. Sin embargo, la fragmentación de la regulación, el riesgo de sufrir ciber-ataques y violaciones de seguridad, las filtraciones masivas de *big data,* o el uso no autorizado de datos biométricos nos llevan a poner en duda el papel predominante que la regulación otorga al consentimiento previo del propietario en la cesión de los datos personales como clave del sistema. En este sentido, las normas de protección de datos generales del nuevo reglamento prohíben el tratamiento de los datos personales relativos a la salud, pero las numerosas excepciones a esta regla general pueden limitar los derechos del interesado. Además, la falta de medidas técnicas y organizativas comunes para garantizar el respeto del principio de minimización de datos y la falta de obligación de aplicar medidas de compatibilidad para intercambiar, cuando sea necesario, los datos obtenidos en los Estados miembros pueden poner en grave riesgo los beneficios de la regulación y amenazar la efectividad del derecho a la privacidad.

New European Regulations on clinical trials, medical devices or the European Regulation on data protection, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, incorporate several rules to ensure the right to privacy and the data protection in the field of health. However, the fragmentation

[*] Artículo recibido el 1 de marzo de 2019 y aceptado para su publicación el 6 de junio de 2019.

of the regulation, the risk of cyber-attacks and security breaches, the massive leaks of big data or the unauthorized use of biometric data, lead us to question about the dominant role that the regulation gives to the prior consent of the owner in the transfer of personal data as a key of the system. In this sense, the rules of protection of general data of the new Regulation prohibit the treatment of the personal data relating to health, but numerous exceptions to this general rule, may limit the rights of the person concerned. In addition, the lack of common technical and organizational measures to ensure the respect of the principle of data minimization and lack of obligation to implement measures of support for exchange, where necessary, the data obtained in the States Members can put at risk the benefits of regulation and threaten the effectiveness of the right to privacy.

Palabras clave / Keywords:

Protección de datos / Big data / Privacidad / Datos de salud / Datos biométricos / Datos genéticos / Huella digital.

Data protection / Big data / Privacy / Health data / Biometric data / Genetic data / Fingerprinting.

1. Introducción y marco normativo

Resulta llamativo que el poder constituyente, en un momento inicial del desarrollo de la era tecnológica, incluyera en el artículo 18 de la Constitución Española de 1978[1] (en adelante CE) un precepto, el único de todo el texto que incluye el término "informática", con la intención de alertar al legislador sobre los peligros que ésta podía representar para el honor y la intimidad de los ciudadanos y le encomendara abiertamente "limitar su uso".

No menos paradójico resulta que el derecho a la protección de la salud previsto en artículo 43 CE, incardinado en el capítulo relativo a los principios rectores de la política social y económica, tiene reservado un nivel de protección menor que el dispensado al derecho a la protección de los datos de salud, aun teniendo en cuenta que, desde el punto de vista funcional, el derecho a la protección de los datos de salud resulta instrumental del primero.

Por mor del artículo 10.2 CE, para interpretar las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce, resulta necesario acudir a la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

[1] El artículo 18.4 CE señala que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229&p=20110927&tn=1#a18

En este sentido, además de la obligada referencia al artículo 12 de la Declaración Universal de Derechos Humanos[2] no podemos evitar citar el acervo comunitario que como miembro de la Unión Europea (en lo sucesivo UE) España ha ido ratificando, además de los textos normativos adoptados en el seno del Consejo de Europa que abordan el campo del derecho a la privacidad e intimidad.

Sin ánimo exhaustivo, resulta obligado aludir a los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[3], el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[4] (CEDH), así como el artículo 10 del Convenio de Oviedo[5], y más recientemente el artículo el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)[6], que abordan, desde diversos puntos de vista, la protección de la vida privada y familiar y la intimidad.

---

[2] En virtud del artículo 12 de la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948 "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Disponible en: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

[3] El artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce a toda persona el derecho al respeto de su vida privada y familiar, su hogar y sus comunicaciones. Mientras que el artículo 8 reconoce a toda persona tiene derecho a la protección de los datos personales que le conciernen. Dichos datos deben procesarse de manera justa para fines específicos y sobre la base del consentimiento de la persona interesada o de alguna otra base legítima establecida por la ley yEveryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. subraya que el cumplimiento de estas reglas estará sujeto al control de una autoridad independiente. Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf

[4] El artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales señala que todos tienen el derecho al respeto por su vida privada y familiar, su hogar y su correspondencia. Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf

[5] El artículo 10 del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997, reconoce a toda persona el derecho al respeto de la vida privada en relación con la información sobre su salud a conocer la información recopilada sobre su salud. Disponible en: https://www.boe.es/boe/dias/1999/10/20/pdfs/A36825-36830.pdf

[6] El artículo 16 del Tratado de Funcionamiento de la Unión Europea, señala que todos tienen derecho a la protección de los datos personales que los conciernen. El Parlamento Europeo y el Consejo, de conformidad con el procedimiento legislativo ordinario, establecerán las normas relativas a la protección de las personas en lo que respecta al tratamiento de datos personales por parte de las instituciones, órganos, oficinas y agencias de la Unión, y por parte de los Estados miembros al realizar actividades que entran en el ámbito de aplicación del Derecho de la Unión, y las normas relativas a la libre

Un escalón por debajo del TFUE, a nivel del derecho derivado, el vigente Reglamento (UE) 2016/679[7] (en lo sucesivo RGPD), pasó a reglar la protección de datos en toda la Unión Europea a partir del 25 de mayo de 2018, aunque exige de desarrollo normativo por parte de los estados miembros en algunos extremos, como más tarde veremos.

En efecto, el RGPD reproduce la arquitectura de la nueva generación de reglamentos europeos que han ido derogando a las directivas aprobadas durante la década de los 90 del siglo pasado, combinando la existencia de preceptos que producen efecto directo, un elemento característico y exclusivo de los reglamentos, con otras previsiones que exigen de una suerte de "transposición impropia" por parte de los legisladores nacionales, como ocurría con las directivas tradicionales.

Dentro de este segundo grupo de previsiones podemos citar a modo de ejemplo, un aspecto tan sensible como la edad mínima fijada en el RGPD en 16 años, para que los menores de edad puedan prestar su consentimiento sin intervención de las personas titulares de la patria potestad o tutela, en relación con los servicios de la sociedad de la información en el artículo 8 RGPD, que puede ser objeto de rebaja mediante ley por parte de los estados miembros hasta un límite de 13 años.

Nada cabe objetar a la remisión que realiza el RGPD a la normativa interna de los Estados Miembros, si bien, el resultado obtenido, desde el punto de vista material, no parece adecuado, toda vez que un menor entre los 13 y los 16 años puede estar facultado o no para prestar consentimiento válidamente en función del país de la UE en el que se encuentre.

En el caso del Reino de España, la recién aprobada Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales[8] (a la que nos referiremos en adelante como LOPD), completa

---

circulación de dichos datos.Compliance with these rules shall be subject to the control of independent authorities. El cumplimiento de estas reglas estará sujeto al control de las autoridades independientes. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=ES

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, y por el que se deroga la Directiva 95/46/CE. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales publicada en el Boletín Oficial del Estado núm. 294

las previsiones del RGPD en el marco del ordenamiento jurídico nacional y desarrolla el contenido mínimo del artículo 18 de la CE fijando en 14 años el límite legal para consentir válidamente.

No obstante, debido a la distribución competencial entre la UE y los estados miembros, el nuevo Reglamento Europeo no resulta de aplicación a la protección de datos en relación con la seguridad de los estados, pero puede incidir en aspectos relacionados con los datos de salud, biométricos o genéticos. De esta forma, la Directiva (UE) 2016/680[9], que también entró en vigor el 25 de mayo de 2018, sirve de marco para la transposición –ahora sí en su modalidad tradicional– en los ordenamientos jurídicos internos de las normas para la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

La citada Directiva contempla en su artículo 10 idénticas garantías a las fijadas por el RGPD en relación con el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física.

Debe recordarse, además que su ámbito subjetivo de aplicación no sólo incluye a los investigados o autores de un delito sino también a sus víctimas reales o potenciales, así como a terceras partes involucradas en una infracción penal como testigos, confidentes o personas de contacto o asociados de eventuales delincuentes o víctimas.

---

de 6 de diciembre de 2018. Disponible en: https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA .Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

Tratándose de un ámbito relacionado con la actividad de investigación y enjuiciamiento de delitos es indudable la presencia en los sumarios de gran cantidad de datos tanto de salud no sólo del eventual autor del delito sino también de la víctima, las secuelas producidas, datos biométricos, tales como huellas, o incluso genéticos, como muestras de ADN del autor o de la víctima.

Por último, la preocupación por la protección de los datos trasluce no sólo en la regulación general contenida en el RGPD sino también en la normativa sectorial sobre cuestiones concretas relacionadas con el Derecho Sanitario. Cabe citar aquí, a modo de ejemplo las previsiones contenidas en el Reglamento (UE) 2017/745, de 5 de abril de 2017, sobre productos sanitarios[10], en relación con la denominada "tarjeta del implante" que contiene información para ser suministrada al paciente con un dispositivo implantado y puede ser solicitada por las autoridades nacionales reglada en el articulo 18, la creación de una base de datos europea sobre dispositivos médicos (Eudamed) prevista en el artículo 26 o la base de datos UDI (Unique Device Identification) que regula el artículo 28 o las previsiones contenidas en el Reglamento (UE) 536/2014, de 16 de abril de 2014 sobre los ensayos clínicos de medicamentos de uso humano[11], para el empleo, por parte de universidades y otros centros de investigación, de datos de ensayos clínicos para su utilización en futuras investigaciones fuera del protocolo del ensayo clínico, previo consentimiento del interesado.

2. Avances tecnológicos y nuevos retos

Frente a un modelo de recopilación y tratamiento de datos que podríamos calificar como pasivo, en el que los datos eran grabados manualmente en soportes físicos locales y raramente eran compartidos[12], la rápida evolución

[10] Reglamento (UE) 2017/745, de 5 de abril de 2017, sobre productos sanitarios, que modifica la Directiva 2001/83/ CE, el Reglamento (CE) nº 178/2002 y el Reglamento (CE) nº 1223/2009 y deroga las Directivas 90/385/CEE del Consejo y 93/42/EEC. Disponible en: https://www.boe.es/doue/2017/117/L00001-00175.pdf

[11] Reglamento (UE) 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0536&from=ES

[12] Este modelo de recopilación de datos aun no estando exento de riesgos ofrecía mayor seguridad que el modelo actual de recopilación masiva de "big data". En este particular puede consultarse Álvarez-Cienfuegos Suárez, José María, *La defensa de la intimidad de los ciudadanos y la tecnología informática,* Ed. Aranzadi, Pamplona, España, 1999, pp. 99-117; Portero Sánchez, Isabel María, "Confidencialidad e informatización en la sanidad", *Derecho y Opinión*, Núm. 6, 1998, pp. 411-420 y Rebollo Delgado, Lucrecio / Serrano Pérez,

técnica, en gran parte desarrollada al albor de las tecnologías móviles, permite que los dispositivos capten datos, de forma autónoma, constante e inadvertida para nosotros gracias a sus sensores y los envíen a través de internet a servidores alojados, en ocasiones, a miles de kilómetros de distancia. Esa ingente capacidad de datos o "big data" es analizada e interpretada de forma articulada a través de complejos algoritmos a los efectos de poder llegar a predecir los comportamientos de las personas, en la mayor parte de los casos, en su faceta como consumidoras[13].

De esta forma, a través de la red circulan todo tipo de datos personales, como identificaciones (número de DNI, Pasaporte) datos bancarios (números de cuentas o tarjetas bancarias, números de cuentas en pasarelas de pago online), fotografías personales[14], nombres de usuario, claves de acceso, o la ubicación exacta a través de la señal de posicionamiento global o GPS de nuestro dispositivo, con los que empresas especializadas pueden identificarnos.

El artículo 4 del RGPD define los llamados "datos personales" como aquellos datos que contienen cualquier información relacionada con una persona física identificada o identificable a la que se denomina "sujeto de datos". Se considera sujeto de datos a toda aquella persona física que puede identificarse, directa o indirectamente, en particular por referencia a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos de los

María Mercedes, *Introducción a la protección de datos,* Ed. Dykinson, Madrid, España, 2008.

[13] Este modelo supondrá sin duda, un mayor impacto para la actividad asistencial. En esta materia, puede consultarse: Goodman, Kenneth W., *Ethics, Medicine and Information Technology: Intelligent Machines and The Transformation of Heatlh Care*, Ed. Cambridge University Press, Cambridge, Reino Unido, 2015.

[14] De acuerdo con el artículo "Facebook's DeepFace software can match faces with 97.25% accuracy" de la revista Forbes, la Compañía Facebook dice haber desarrollado un software de reconocimiento facial denominado "DeepFace" que, a través de las etiquetas de otros usuarios y sin la previa autorización del sujeto, permite identificar a sujetos en fotografías con un 97.5% de certeza. Disponible en: https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#3c001e4654fc. En el lado opuesto, el experimento desarrollado por la American Civil Liberties Union (UCLA por sus siglas en inglés) ha alertado sobre los problemas de este tipo de sistemas de seguridad, al demostrar que el software "Rekognition" comercializado por la empresa Amazon, confundió los rostros de 28 congresistas federales de Estados Unidos con los rostros de criminales incluidos en una base de datos con 25.000 fotografías de delincuentes. Los resultados del experimento están disponibles en: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

factores físicos, fisiológicos, identidad genética, mental, económica, cultural o social de esa persona natural.

Bajo la premisa de la disponibilidad de dichos datos en nuestro dispositivo móvil en todo momento y lugar, compartimos todo tipo de información a través de la red y consentimos la recopilación masiva de datos acerca de nuestra persona.

En la mayor parte de los casos, se trata de datos personales relacionados con el estilo de vida o *lifestyle*. En otros casos, esos datos sobre estilo de vida pueden ser relevantes a los efectos de deducir o predecir comportamientos del sujeto. En este sentido, abundan aplicaciones ofrecidas de forma gratuita por numerosas compañías que comercializan seguros de vida y de salud que, dicen fomentar hábitos de vida saludable y a cambio de descuentos en las primas, monitorizan la actividad de sus asegurados[15] (número de pasos, escaleras ascendidas, horas de sueño, etc).

Otras aplicaciones van más allá, y pueden recabar datos acerca de nuestra voluntad de dejar de fumar (monitorizando las horas y el número de cigarrillos que fumamos diariamente) o incluso tener un bebé (monitorizando el ciclo menstrual o aspectos tan íntimos como las relaciones sexuales mantenidas durante el mismo).

Junto a estos datos, se ha extendido el uso de nuestra huella digital única y personal, nuestro rostro o el iris de los ojos para bloquear o desbloquear nuestros dispositivos de forma más rápida y sobre todo "segura".

Así pues, los dispositivos son capaces de leer y almacenar datos biométricos, definidos por el RGPD como los datos personales resultantes de un procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de esa persona física, como imágenes faciales o datos dactiloscópicos, como la huella dactilar.

[15] A modo de ejemplo, combinando datos conocidos a través de la póliza como el horario destinado a la actividad profesional, la edad o el estado civil del asegurado con otros datos proporcionados por las aplicaciones como son las horas de sueño o los pasos durante las noches de los fines de semana, pueden extraerse conclusiones en relación con el tiempo de ocio o los hábitos del asegurado. De esa forma, pueden hacerse predicciones acerca de la probabilidad de que un determinado estilo de vida incida en su salud, y consecuentemente del riesgo que corre la compañía aseguradora.

Algunas empresas van más allá y afirman que disponen de programas que además de identificar a una persona empleando una fotografía de su rostro pueden conocer, a través de ella, aspectos relativos a su personalidad, los sentimientos, la salud mental y prever el comportamiento del sujeto[16].

En este punto, la Directiva 2016/680 prohíbe, en el ámbito policial y penal, la toma de decisiones basadas únicamente en un tratamiento automatizado, a través de lo que se ha denominado "Inteligencia Artificial", incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, si bien, de forma inquietante advierte de la posibilidad de que, en un futuro, la normativa de la UE o la interna de los Estados autorice la toma de decisiones basadas en inteligencia artificial.

El uso de datos biométricos permite identificarnos sin ningun género de duda en las redes sociales en la que manifestamos nuestros gustos, aversiones, preferencias, opiniones o inclinaciones políticas, condición sexual o sentimientos religiosos, entre otros.

Tal y como ha señalado la Agencia Española de Protección de Datos[17] (en adelante AEPD), la recopilación de los datos biométricos debe estar presidida por el principio de proporcionalidad. La AEPD consideró que "el tratamiento del sistema de huellas para acceder a un establecimiento exige una especial atención a la proporcionalidad, no solo por el carácter excesivo en la recogida sino en la modalidad técnica para tratarlo reiteradas veces, es decir que el dato que figure en sus sistemas sea objeto de tratamiento en tanto resulte completamente imprescindible para el cumplimiento de la finalidad perseguida, la de autenticar la entrada al gimnasio".

---

[16] El informe "AI Now Report 2018" del Instituto de Investigación A.I. Now de la Universidad de Nueva York alerta del llamado "reconocimiento de afecto" que es una subclase de reconocimiento facial que pretende detectar aspectos relativos a la personalidad, los sentimientos internos, la salud mental de cualquier sujeto y el "compromiso del trabajador" basado en imágenes o videos de caras, con base en razonamientos que a menudo recuerdan a pseudociencias como la frenología y la fisonomía. Denuncian que estas técnicas no están respaldadas por evidencia científica sólida, y se están aplicando de manera no ética e irresponsable, en relación con la contratación laboral, el acceso a seguros, educación y vigilancia, por lo que abogan por la aprobación de leyes nacionales que requieran una supervisión estricta, limitaciones claras y transparencia pública sobre el software de reconocimiento facial. Disponible en: https://ainowinstitute.org/AI_Now_2018_Report.pdf

[17] Resolución de la AEPD 900/2018. Disponible en: https://www.aepd.es/resoluciones/PS-00002-2018_ORI.pdf

Recientemente, la AEPD[18] ha advertido de la huella digital o "fingerprinting" que nuestro dispositivo deja cuando navegamos por la red concluyendo que "las técnicas de *fingerprinting* recogen datos del equipo del usuario, de forma general, sin su conocimiento ni consentimiento, tratando información sobre las características del terminal, en algunos casos con una finalidad distinta del propósito técnico inicialmente previsto, mediante la ejecución en el terminal de aplicaciones que captan y transmiten datos hacia los servidores del responsable del tratamiento. El conjunto de datos recabados puede ser tan extenso, o enriquecerse de tal forma, que identifique unívocamente al usuario, y entre los mismos se pueden encontrar algunos definidos como de categoría especial según el RGPD. Este conjunto es, a priori, desconocido, se plantean serias dudas sobre la aplicación del principio de minimización de datos, así como del periodo durante el cual son almacenados. No se proporcionan herramientas para poder evitar la recogida de datos, ya que una vez iniciado el acceso la página en internet, y antes de que el usuario haya podido visualizarlo, el servidor ya tiene toda la información de su fingerprint. Incluso se han detectado casos en los que, de forma general, no se atiende a la configuración DNT (*Do Not Track*) establecida por el usuario para desactivar la recogida de la huella digital en los servicios de Internet. No se cumple con la obligación de obtener el consentimiento informado y, en particular, respecto a la finalidad para la que se recaban los datos, ya que dichas técnicas se utilizan generalmente para realizar perfilado del usuario (entre las cuales cabe la toma de decisiones con consecuencias sobre el servicio) y analizar su actividad en internet. El usuario no dispone de medios para ejercer los derechos establecidos en el RGPD cuando se recogen o asocian a datos personales".

A todos estos avances, recientemente se han sumado una serie de dispositivos designados genéricamente con el vocablo anglosajón "wearables" que pueden controlar variables como la presión arterial, la frecuencia cardíaca, los porcentajes de oxígeno en sangre, el pulso, los pasos diarios, el número de horas y la calidad de nuestro sueño y volcar los datos en la red a tiempo real.

No cabe duda que dichos parámetros forman parte de los datos de salud en los términos establecidos en el RGPD cuando los define como aquellos datos personales relacionados con la salud física o mental de una persona física, incluida la prestación de servicios de asistencia sanitaria, que revelan información sobre su estado de salud.

[18] AEPD "Estudio fingerprinting o Huella digital del dispositivo". Disponible en: https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf

Combinando varios de los datos de salud proporcionados por estos dispositivos podemos conocer otros datos como el estado basal[19] en el que influyen de forma notable aspectos genéticos de un sujeto, o incluso la presencia de patologías o malformaciones congénitas del portador del dispositivo. Todos estos aspectos nos proporcionan "datos genéticos", ya que afectan a las características genéticas heredadas o adquiridas de una persona física y proporcionan información única sobre la fisiología o la salud de esa persona física y que resultan, en particular, de un análisis de una muestra biológica de tal persona en cuestión.

3. El consentimiento del sujeto como clave del sistema

A todos nos resulta conocida la frase "una cadena es tan fuerte como su eslabón más débil". Ello nos lleva a cuestionarnos si los ciudadanos conocen el alcance de la cesión de los datos cuando aceptan su tratamiento a través del consentimiento de las llamadas cláusulas de privacidad.

El Eurobarómetro 431[20] publicado en 2015 acerca de la protección de datos en la Unión Europea nos ofrece datos esclarecedores sobre esta materia, concluyendo que solo una minoría (15%) siente que tiene control total sobre la información que proporciona en línea, el 31% de los encuestados piensa que no tiene ningún control sobre dichos datos, dos tercios de los encuestados (67%) están preocupados por no tener un control completo sobre la información que proporcionan en línea. La mayoría de los encuestados están preocupados por la grabación de sus actividades a través de tarjetas de pago y teléfonos móviles (55% en ambos casos), solo dos de cada diez encuestados están siempre informados sobre la recopilación de datos y la forma en que se utilizan los datos, solo una quinta parte de los encuestados lee completamente las declaraciones de privacidad (18%). Nueve de cada diez europeos piensan que es importante para ellos tener los mismos derechos y protección sobre su información personal, independientemente del país en el que se basa la autoridad pública o la compañía privada que ofrece el servicio, más de cuatro de cada diez encuestados (45%) piensan que la aplicación de las normas sobre protección de datos personales debe tratarse a nivel europeo,

[19] Puede ser definido como el estado del organismo en reposo con un gasto mínimo de energía para el mantenimiento de la respiración y otras funciones vegetativas. El estado basal a menudo puede estar relacionado con la carga genética del sujeto.

[20] Eurobarómetro especial 431 sobre protección de datos publicado en Junio de 2015 disponible en: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf y Eurobarómetro 443 publicado en diciembre de 2016 sobre privacidad publicado en: http://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG

mientras que una proporción ligeramente inferior (42%) cree que debería tratarse a nivel nacional. Más de la mitad de las personas que usan las redes sociales en línea han intentado cambiar su configuración de privacidad, tres cuartas partes de las personas que intentaron cambiar su configuración de privacidad dijeron que el proceso fue fácil, mientras que las personas que no han cambiado sus configuraciones de privacidad son más propensas a decir que no lo consideran necesario o que no saben cómo hacerlo.

En 2014, la Agencia Europea Europol participó en el experimento llevado a cabo por un grupo de investigadores de seguridad que instaló un punto de conexión wifi gratuito en Londres. Cuando las personas se conectaban al punto de acceso, los términos y condiciones que se les pedía que firmaran incluían una "cláusula de Herodes" que prometía Wi-Fi gratuito, pero solo si "el destinatario aceptaba ceder a su primer hijo durante la eternidad a la empresa suministradora de la conexión[21]". Seis personas se registraron aunque afortunadamente, la empresa que realizó el experimento confirmó que no ejecutarían la cláusula contractual.

Con carácter general, según el párrafo 1 del artículo 9 del RGPD, se prohíbe el procesamiento de datos personales que revelen datos genéticos, datos biométricos con el fin exclusivo de identificar a una persona física, o relativos a la salud.

Sin embargo, el reconocimiento de nada menos que diez excepciones del párrafo 2 que permiten levantar dicha prohibición, distorsionan el sistema de protección a efectos prácticos. No resulta neutral que el consentimiento explícito del interesado al tratamiento de esos datos personales para uno o más fines específicos sea una excepción a dicha prohibición, excepto cuando la legislación de la Unión o del Estado miembro establece que la prohibición mencionada en el párrafo 1 no pueda ser anulada.

En este punto, el artículo 9 de la LOPD regula determinadas categorías especiales de datos, y únicamente establece que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. No así en el caso del tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada,

[21] The guardian "Londoners give up eldest children in public Wi-Fi security horror show". Disponible en: https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause

o la ejecución de un contrato de seguro del que el afectado sea parte, para lo que deberá a estarse a una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En este punto, la LOPD permite que el consentimiento del sujeto levante la prohibición de tratamiento de los datos de salud, pero difiere a una futura "norma con rango de Ley" la regulación del tratamiento de datos en el ámbito de la salud.

Dos objeciones cabe formular a dicha regulación, la primera tiene que ver con el escaso o nulo valor del consentimiento prestado online, cuando el sujeto de los datos se enfrenta, en la mayor parte de las ocasiones, a un deliberadamente farragoso listado de cláusulas de privacidad[22] que debe limitarse a aceptar antes de acceder a un determinado contenido. La experiencia nos ha demostrado que la mayor parte de los usuarios no son capaces de comprender el alcance de dichas cláusulas o directamente las acepta sin apenas leer su contenido.

La segunda objeción tiene un alcance meramente formal, y se refiere a la técnica normativa aplicada por el legislador en este punto. Aunque es de agradecer que la LOPD indique que la norma que regule la protección de datos en materia de salud tenga rango de ley, de nada sirve que una Ley Orgánica, realice una remisión a otra norma posterior que desconozca el contenido de un precepto de rango superior como es el artículo 81 CE.

La regulación de la protección de unos datos tan sensibles como los de salud no debe realizarse mediante una ley ordinaria ya que, como hemos visto, supone el desarrollo del contenido esencial del derecho a la intimidad personal y familiar reconocido en el artículo 18 de la CE.

En consecuencia, se trata de una norma relativa al desarrollo de un derecho fundamental y, por tanto, la regulación de su contenido esencial no puede realizarse por otra norma que no sea una Ley Orgánica. El Tribunal Constitucional ya se ha pronunciado en algunas ocasiones acerca de la necesidad de respetar la reserva de Ley Orgánica en la regulación de los derechos

[22] En septiembre de 2017 la AEPD multó a Facebook con 1,2 millones de euros en España por infringir las leyes de privacidad. En la resolución la AEPD manifestó que –"la política de privacidad de Facebook contiene términos genéricos y poco claros", –"Facebook no recopila adecuadamente el consentimiento de sus usuarios o no usuarios, lo que constituye una infracción grave". –"El usuario medio de Facebook no está al tanto de cómo la empresa recopila, almacena y usa sus datos".

y libertades, declarando inconstitucionales preceptos que infringieron dicha reserva[23].

En el caso de la oferta de servicios de la sociedad de la información directamente a un niño, de conformidad con el artículo 8 del Reglamento, los Estados miembros pueden establecer por ley una edad inferior a la regla general de 16 años, con un límite de 13 años.

El artículo 7 de la LOPD establece que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. Mientras que, para el tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determine este último.

Con independencia de la valoración que merezca la disparidad en la regulación europea o la rebaja en dos años de la edad mínima para prestar consentimiento válido contenida en la LOPD, cabe reseñar que por fin se ha elevado al rango de Ley Orgánica un precepto contenido en el aún vigente, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aprobado por Real Decreto 1720/2007, de 21 de diciembre[24].

4. La seguridad de los datos como presupuesto básico

Uno de los presupuestos en los que fundar el otorgamiento de un consentimiento válido es el relativo a la previa información acerca de las

[23] Cabe traer a colación, en este punto, las sentencias del Tribunal Constitucional 131/2010 y 132/2010, de 2 de diciembre de 2010 que declararon inconstitucionales, pero no nulos, los artículos 211 del Código civil y 763.1 de la Ley 1/2000, de 7 de enero, de enjuiciamiento civil por quebrar la reserva de ley orgánica, regulando mediante ley ordinaria, del internamiento forzoso en establecimiento de salud mental de quienes padezcan trastornos psíquicos como limitación a la libertad personal. Disponibles en: https://www.boe.es/boe/dias/2011/01/05/pdfs/BOE-A-2011-273.pdf y https://www.boe.es/boe/dias/2011/01/05/pdfs/BOE-A-2011-274.pdf

[24] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal publicado en el BOE núm. 17, de 19 de enero de 2008. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

garantías que ofrece el encargado del tratamiento o custodia de los datos. No puede entenderse que un sujeto consienta el tratamiento de sus datos si no se le informa adecuadamente de quiénes van a tener acceso a los mismos a través de la cesión de los mismos por el encargado del tratamiento o de las medidas de seguridad concretas de las que dispone para impedir el acceso no autorizado a los mismos. Debemos plantearnos si la seguridad en la custodia de los datos debe resultar un presupuesto habilitante para el intercambio de datos y para el otorgamiento de consentimiento.

La Comisión Europea señaló en enero de 2016[25] que las empresas de la UE que ofrecen servicios amigables con la privacidad pueden ser más atractivas para los consumidores y, por lo tanto, más competitivas. Concluyó que "la UE tiene los más altos estándares de protección de datos en el mundo. Esto genera confianza".

Las redes sociales se han convertido recientemente en protagonistas de titulares en relación con brechas de seguridad o incluso filtraciones deliberadas de datos personales. Por ejemplo, en mayo de 2017 la Unión Europea multó a Facebook con 110 millones de euros por infringir las leyes de protección de datos y por los reguladores engañosos durante su adquisición de WhatsApp, que según dijo no estaría vinculado a la red social[26].

Apenas un año después, en mayo de 2017, el ataque de ramsomware "WannaCry" golpeó a muchas instituciones y corporaciones, pero especialmente al Servicio Nacional de Salud (NHS) de Inglaterra, bloqueando el acceso por parte del personal a las bases de datos de sus computadoras y obligando a derivar a sus pacientes a hospitales en los que se pudiera acceder a su historia clínica[27]. Por primera vez fuimos conscientes que un ataque que bloqueara los datos de salud era capaz de sobrepasar las fronteras del mundo virtual y traducirse en un problema sanitario de primer nivel originando un

---

[25] Dirección General de Justicia y Consumidores de la Comisión Europea "The EU Data Protection Reform and Big Data", *Factsheet,* Enero 2016. Disponible en: ec.europa.eu/newsroom/just/document.cfm?doc_id=41523

[26] El 15 de marzo de 2018, la AEPD impuso otra sanción de 600.000 euros a las empresas Whatsapp y Facebook (300.000 a cada una) por cesión y tratamiento de datos personales de sus usuarios sin consentimiento de los sujetos.

[27] Más tarde fue conocido que WannaCry se propagó gracias a una vulnerabilidad en Microsoft, que había sido subsanada a través una actualización lanzada en marzo de ese mismo año. Sin embargo, las personas no siempre instalan actualizaciones y parches en sus computadoras, lo que significa que las vulnerabilidades pueden permanecer abiertas por mucho más tiempo y facilitar el acceso de los hackers.

caos organizativo en uno de los sistemas nacionales de salud con mayor prestigio.

Nadie está exento de vulneraciones en su seguridad. De hecho, en agosto de 2017 el Ministerio de Justicia Español confirmó la filtración de 11.000 documentos alojados en un servidor accesible desde Internet. Entre la información filtrada había datos extremadamente sensibles como los contenidos en la base de datos Orfila, el sistema que comunica los Tribunales, Fiscalías y Registro Civil con los Institutos Españoles de Medicina Legal, y en el que se contienen, entre otros, datos de salud (resultados de pruebas periciales o autopsias) y datos genéticos (análisis de ADN).

El artículo 32 del RGPD determina que los sistemas de seguridad deben ser implementados bajo los siguientes criterios, el estado del arte, los costos de implementación, y la naturaleza, el alcance, el contexto y los fines del procesamiento, así como el riesgo de variabilidad y gravedad de los derechos y libertades de las personas físicas.

Según el artículo 34, cuando la violación de los datos personales pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas, el responsable deberá comunicar la violación de los datos personales al interesado sin demoras indebidas a menos que implique un esfuerzo desproporcionado. En tal caso, deberá haber una comunicación pública o una medida similar mediante la cual se informe a los interesados de manera igualmente efectiva.

En resumen, un aspecto clave como es la seguridad de los datos de salud, puede estar sometida a variables tan difusas como los "costos de implementación" o la necesidad de acometer un "esfuerzo desproporcionado". La seguridad de los datos debe estar garantizada en un momento anterior a su recopilación y tratamiento y no puede verse limitada por los costos de su mantenimiento.

5. Conclusiones

Aunque formalmente el objetivo del nuevo RGPD es proporcionar más control al ciudadano sobre los datos, el Eurobarómetro 431 muestra que los ciudadanos europeos no están familiarizados con la política de privacidad de las empresas y reconocen que no tienen ningún tipo de control sobre los datos que les transfieren.

Las grandes empresas, están dando muestras de su interés en el ámbito sanitario[28], y ya están desarrollando dispositivos y aplicaciones móviles para recabar ingentes cantidades de datos y ofrecer acceso a las historias clínicas de miles de pacientes. La reciente normativa no da respuesta al rápido avance de las tecnologías al otorgar un peso excesivo al consentimiento del interesado.

Pese al notable avance en el camino de la armonización de la regulación común en los estados miembros que supone el empleo de un Reglamento en lugar de una Directiva como instrumento jurídico, las remisiones a la normativa interna de los estados que realiza el RGPD en diversas materias (a modo de ejemplo, la edad mínima para prestar consentimiento en el caso de sujetos especialmente vulnerables como son los menores edad), produce inequidades en la protección del derecho en función del país en el que se encuentre el sujeto de datos.

Junto a la seguridad de los datos, debe ahondarse en su interoperabilidad, especialmente los relativos a la salud. La UE está fomentando modelos de historiales médicos electrónicos que cumplan normas estrictas de protección de los datos sanitarios y de seguridad de las redes y los sistemas de información en los que se basan dichos sistemas garanticen un acceso seguro a los sistemas a fin de evitar violaciones de la seguridad de los datos y minimizar los riesgos de incidentes de seguridad y conmina a los Estados miembros a que garanticen que los ciudadanos y los profesionales sanitarios tengan acceso en línea a sus historiales médicos electrónicos utilizando medios de identificación electrónica segura[29].

Las sanciones económicas no persuaden a las grandes empresas a infringir la regulación en materia de protección de datos, siempre que sea más rentable pagar una sanción que cumplir con la regulación. Como lamentablemente hemos visto, la seguridad de los datos es la clave de la confianza. Debe gobernar, sin excepción sobre otros criterios.

Cabe concluir al fin que no siempre el reconocimiento de más derechos para los ciudadanos se traduce en un mayor control. Las autoridades públicas

---

[28] Eldiario.es "Cuando las grandes tecnológicas quieren tu historial médico: así están invirtiendo en salud Apple, Microsoft, Amazon y Google", Disponible en: https://www.eldiario.es/tecnologia/tecnologicas-Apple-Microsoft-Amazon-Google_0_847965532.html

[29] Recomendación (UE) 2019/243 de la Comisión de 6 de febrero de 2019 sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019H0243&from=EN

independientes deben ser los actores principales en la atención del interés de los ciudadanos y tener un papel activo en la lucha contra el abuso de algunas empresas, asegurando que el consentimiento explícito ha sido prestado con información suficiente y comprensible. Esta obligación viene impuesta desde el punto de vista normativo en el artículo 16 TFUE cuando señala que "el cumplimiento de estas reglas estará sujeto al control de las autoridades independientes".

6. Bibliografía

Álvarez-Cienfuegos Suárez, José María, *La defensa de la intimidad de los ciudadanos y la tecnología informática,* Ed. Aranzadi, Pamplona, España, 1999.

Goodman, Kenneth W., *Ethics, Medicine and Information Technology: Intelligent Machines and The Transformation of Heatlh Care,* Ed. Cambridge University Press, Cambridge, Reino Unido, 2015.

Portero Sánchez, Isabel María, "Confidencialidad e informatización en la sanidad", *Derecho y Opinión*, Núm. 6, 1998.

Rebollo Delgado, Lucrecio / Serrano Pérez, María Mercedes, *Introducción a la protección de datos,* Ed. Dykinson, Madrid, España, 2008.

Utilización de tecnología *Big Data* en investigación clínica*

Use of Big Data technology in clinical research

Guillermo Alcalde Bezhold

Comité Ético de Investigación Clínica. Organización Sanitaria Integrada Araba (Vitoria, España)

Iciar Alfonso Farnós

Comité de Ética de la Investigación con medicamentos de Euskadi, Dirección de Farmacia, Gobierno Vasco (Vitoria, España)

DOI: 10.14679/1133

Sumario / Summary: 1. Introducción. 2. *Big Data* e inteligencia artificial. 3. Generación de datos en la práctica clínica. 4. Oportunidades del *Big Data* sanitario para las organizaciones sanitarias. 5. Oportunidades del *Big Data* Sanitario en medicina personalizada. 6. Riesgos y limitaciones de la tecnología *Big data*. 7. Retos futuros del *Big Data* en la práctica clínica. 8. Experiencias de *Big Data* con grandes bases de datos sanitarios. 9. Aplicación de la tecnología *Big Data* a la investigación clínica. 10. Limitaciones de la investigación con *Big Data*. 11. Principios éticos en la investigación con *Big Data*. 12. Control ético y legal de los proyectos *Big Data*. 13. La utilización de datos anonimizados. 14. Conclusiones. 15. Bibliografía.

Resumen / Abstract: La utilización de la tecnología *Big data* en la práctica clínica puede suponer grandes avances para el sistema sanitario, tanto para la asistencia

---

* Artículo recibido el 5 de junio de 2019 y aceptado para su publicación el 16 de julio de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos –*Big Data*–. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

como para la investigación clínica. Para conseguir este objetivo es imprescindible la integración de las diferentes fuentes de información actualmente disponibles. De forma simultánea a estas ventajas potenciales, la aplicación de estas tecnologías puede suponer una fuerte amenaza para la intimidad, por lo que es imprescindible disponer de medidas adecuadas de control de la información, así como implantar procedimientos adecuados, transparentes y seguros, que garanticen el máximo nivel de confidencialidad asegurando el respeto a los derechos y libertades de las personas. Para poder utilizar de forma segura esta tecnología es imprescindible disponer de un marco ético y jurídico adecuado, que permita compaginar la protección de datos con la investigación clínica relevante y la mejora de la asistencia.

The use of Big data technology in clinical practice can mean great advances for the healthcare system, both for care and for clinical research. To achieve this goal, it is essential to integrate the different sources of information currently available. Simultaneously with these potential advantages, the application of these technologies can pose a strong threat to privacy, so it is essential to have adequate control measures for information, as well as to implement adequate, transparent and secure procedures, which guarantee the highest level of confidentiality ensuring respect for the rights and freedoms of individuals. In order to be able to use this technology safely, it is essential to have an adequate ethical and legal framework that allows data protection to be combined with relevant clinical research and improved care.

Palabras clave / Keywords:

Investigación clínica / Grandes cantidades de datos / Inteligencia artificial / Asistencia sanitaria.

Clinical research / Big Data / Artificial intelligence / Health care.

1. Introducción

El *Big Data* sanitario es una tecnología que se ha incorporado con fuerza al sector sanitario porque supone una gran fuente de oportunidades para la asistencia y la investigación. Sin embargo, como cualquier otro avance tecnológico, su implantación no está exenta de amenazas. El objetivo de esta revisión es analizar las controversias que han surgido de la aplicación de esta tecnología al sector sanitario y cómo se pueden compaginar las ventajas y los posibles inconvenientes.

Existen múltiples definiciones de lo que representa la tecnología *Big Data*. Una definición habitualmente aceptada es "el acceso a grandes cantidades de información disponible con el fin de dar valor añadido a su análisis integrado, con el objetivo de extraer información oculta o correlaciones imprevistas, no deducibles ni inferibles con los métodos de análisis convencionales" (1).

Otras definiciones del *Big Data* se centran más en la tecnología empleada que en el uso que se da al análisis de los datos. Entre estas tecnologías se

incluyen las diferentes variantes de la inteligencia artificial, que se clasifican según la necesidad de intervención humana, progresivamente menor según avanza la tecnología computacional. Todas estas tecnologías parten del análisis de datos a gran escala a partir del cual se diseñan modelos informáticos.

El *Big Data* sanitario también se caracteriza por reunir las siguientes características claves (3 uves): volumen de los datos; velocidad de procesamiento y variedad de las fuentes. Posteriormente, se han añadido otras características relevantes que deben reunir los datos, como que sean veraces o aporten valor (5 uves) (1,2). Por tanto, no existe una única definición de *Big Data*, sino definiciones que abordan diferentes aspectos complementarios.

La aplicación de la tecnología *Big Data* para el sector sanitario puede ser una fuente generadora de recursos económicos, ligados al conocimiento que generan los datos y las tecnologías para su procesamiento y análisis, de tal forma que se ha atribuido a los datos el papel del nuevo petróleo de la economía digital. Como ejemplo de la importancia de esta tecnología, la Unión Europea ha elaborado el documento "Redesigning health in Europe for 2020", en el que se plantean los grandes retos de la Unión Europea en la aplicación del *Big Data* sanitario (3):

- Incrementar el conocimiento de los ciudadanos sobre las oportunidades de la salud digital (eHealth).

- Generar recursos ligados a la salud digital, entendido como la aplicación de tecnologías digitales de la información y comunicación para mejorar la salud.

- Mejorar la salud de la población, reducir las desigualdades sociales o aumentar la eficiencia del sistema sanitario.

- Fomentar la integración de datos en grandes sistemas europeos y mejorar las posibilidades de acceso para los investigadores, así como conseguir una mayor integración entre la investigación y la práctica clínica.

Por otra parte, el avance progresivo de la tecnología de procesamiento de datos ha supuesto que cada vez sea más factible reidentificar los datos anonimizados, de tal manera que el principio de la utilización de datos anónimos como garantía absoluta de protección de la privacidad ha dejado de ser válido (4). Como ejemplo, se pueden citar estudios previos que han demostrado

que combinando datos básicos del censo de EEUU, tales como la fecha de nacimiento, el sexo y el código postal de residencia, el 87% de la población tiene características únicas, y por tanto identificables (5). De este modo, datos que inicialmente parecen anónimos se pueden reidentificar posteriormente de forma directa mediante la combinación de valores de diferentes variables individuales o mediante el cruce adicional con otras bases de datos relacionadas (4).

2. *Big Data* e inteligencia artificial

La **inteligencia artificial** es una rama de la informática dedicada a crear sistemas que realizan tareas que normalmente requieren la intervención de la inteligencia humana.

Los primeros fundamentos de inteligencia artificial consistían únicamente en la programación por un informático mediante unas reglas preestablecidas según el criterio de expertos sin que interviniese el sistema informático (6). Estas técnicas basadas en la programación eran efectivas en entornos con reglas formales y abstractas (como los programas capaces de jugar al ajedrez), pero se enfrentaban a limitaciones importantes en situaciones intuitivas y sencillas para cualquier persona como reconocer imágenes o entender una conversación. Por este motivo, pronto se llegó a la conclusión de que los sistemas de inteligencia artificial necesitaban tener la capacidad de adquirir su propio lenguaje extrayendo patrones a partir de los datos sin procesar, capacidad denominada aprendizaje de máquina *(*machine learning*)*.

Los primeros sistemas de "machine learning" confiaban en expertos humanos para clasificar las características relevantes a partir de las cuales se entrenaba el sistema, bien fuesen datos o imágenes, como ha ocurrido con los programas capaces de diagnosticar la retinopatía diabética a partir de imágenes clasificadas previamente por oftalmólogos.

Posteriormente, se han incorporado los sistemas denominados de aprendizaje por representación *(representation learning)*, que consisten en algoritmos que aprenden a extraer las características relevantes a partir de los datos sin que se hayan definido previamente por un experto humano.

Por último, los modelos más avanzados de inteligencia artificial se han basado en las técnicas de aprendizaje profundo *(deep learning)* mediante redes neuronales, en las que las características que aprende la máquina son compuestas o jerárquicas en varios niveles, de lo simple a lo más complejo,

sin que el modelo tenga ningún tipo de supervisión humana. Estos sistemas tienen el inconveniente de que no se puede explicar cómo llega el sistema a sus conclusiones, funcionando como una "caja negra" cuya lógica interna es difícil de entender e interpretar para los profesionales expertos en la materia, aunque la predicción sea igual de precisa (7,8,9,10).

Los modelos "deep learning" han tenido gran éxito en diferentes campos, como en la clasificación de imágenes médicas, en el reconocimiento del lenguaje o en el procesamiento del lenguaje natural. Los modelos más complejos de aprendizaje por redes neuronales tienen su campo de acción principal en las especialidades que utilizan imágenes de forma masiva.

De este modo, estas técnicas se han incorporado a la práctica clínica diaria mediante ayudas al diagnóstico, simplificando tareas como la interpretación automática de los electrocardiogramas, el recuento celular de los hemogramas, la lectura automática de citologías vaginales, la interpretación de retinografías para la detección de retinopatía diabética, la detección de pólipos de colon o microsangrados cerebrales en imágenes radiológicas o la interpretación de fotografías para el diagnóstico de cáncer cutáneo, en ocasiones con mejor exactitud que médicos especialistas (7,11).

Por otra parte, también se han desarrollado modelos predictivos mediante sistemas de aprendizaje profundo a partir de los datos de la historia clínica electrónica, que han demostrado su utilidad para predecir la mortalidad durante el ingreso, el riesgo de reingreso no programado a los 30 días, la prolongación de la estancia y los diagnósticos al alta (12). En un futuro, la integración de estas técnicas con herramientas de apoyo a la decisión clínica, tales como alertas automáticas o ayudas al diagnóstico, podrá ofrecer a los médicos información relevante en tiempo real para mejorar las decisiones clínicas (13).

3. Generación de datos en la práctica clínica

La práctica clínica genera diariamente una enorme cantidad de información relevante para conocer la incidencia, prevalencia y evolución de las enfermedades. El desarrollo de la historia clínica electrónica en cada sistema de salud, como repositorio de toda la información asistencial con un identificador único por paciente que enlaza las diferentes bases de datos, ha facilitado el acceso a esta enorme cantidad de información, que según su posibilidad de procesamiento ulterior se puede considerar como estructurada o no estructurada (14).

La historia clínica contiene información estructurada en forma de datos codificados o numéricos que se pueden procesar directamente, como los resultados de laboratorio o las constantes clínicas de los pacientes (temperatura, frecuencia cardiaca o presión arterial). En otras ocasiones, los datos requieren una labor previa de codificación, como ocurre con la codificación de los diagnósticos y procedimientos de cada episodio asistencial mediante sistemas de codificación estándar, de los cuales el utilizado habitualmente es la Clasificación Internacional de Enfermedades (CIE), promovida por la Organización Mundial de la Salud. La codificación mediante la CIE permite convertir los diagnósticos, procedimientos y otros problemas de salud en códigos alfanuméricos homogéneos internacionalmente, lo que facilita su almacenamiento y posterior recuperación para el análisis de la información (15). A partir de la codificación según la CIE se han desarrollado herramientas de análisis de la información asistencial, tales como los GRD (Grupos relacionados con el diagnóstico), que agrupan los episodios de hospitalización por diagnósticos al alta relacionados con un similar consumo de recursos. Estas herramientas son capaces de aportar a los Sistemas de Salud información comparativa de la eficiencia de la actividad clínica (16). Sin embargo, la codificación clínica es un proceso complejo que requiere personal entrenado.

Otros ejemplos de información estructurada son los datos administrativos de los contactos con el sistema sanitario (atenciones en consultas externas, urgencias, hospital de día o ingresos hospitalarios) o los datos obtenidos de los sistemas de prescripción electrónica. Estos datos, cruzados con otra información estructurada como las variables sociodemográficas (edad, sexo o lugar de residencia) y con la codificación de los diagnósticos y/o procedimientos pueden proporcionar información muy valiosa sobre el pronóstico y el manejo de diferentes enfermedades.

En otras ocasiones se ponen en marcha registros específicos para tener un conocimiento exhaustivo de algunas enfermedades o condiciones con especial relevancia para la salud pública. Un registro es un sistema organizado para la recopilación, almacenamiento, extracción, análisis y diseminación de la información sanitaria. En el entorno sanitario se pueden mencionar los ejemplos de los registros de mortalidad, los registros de cáncer, las enfermedades de declaración obligatoria o más recientemente, los registros de enfermedades raras (17).

Pero la práctica clínica genera una cantidad aún mayor de información no estructurada. Los evolutivos o los informes en texto libre de las historias clínicas electrónicas son una fuente no estructurada de información, cuya

finalidad principal es garantizar que los profesionales sanitarios tengan la información clínica disponible para la asistencia y la puedan interpretar según su criterio. La información en texto libre no es directamente procesable, por lo que para que pueda convertirse en información de utilidad para la toma de decisiones y la investigación clínica son necesarios sistemas automáticos capaces de extraer y procesar esta información. Hoy en día se están desarrollando estas herramientas informáticas con el objetivo de tener conocimiento sobre los resultados y la eficiencia de los procesos asistenciales. Eventualmente, estas herramientas podrían ser capaces de detectar patrones de comportamiento clínico y sugerir cursos de acción mientras se está llevando a cabo la asistencia, comparando las características del paciente que se está atendiendo con patrones previos. Sin embargo, los clínicos deberán tener en cuenta que los resultados que se obtienen no dejan de ser predicciones estadísticas y mantener un alto índice de sospecha sobre su exactitud (11).

Existen, por otro lado, otras fuentes de información no estructurada como las imágenes médicas, tanto de pruebas complementarias (radiología, ecografía, medicina nuclear, resonancias, electrocardiografía, retinografías, etc), como fotografías que se adjuntan a la historia clínica. También se incluyen en este apartado las grabaciones en video de procedimientos (2) o incluso la información contenida en las publicaciones científicas, que ha aumentado de forma exponencial en los últimos años (18).

Por último, cada vez van a ser más importantes las fuentes de información alternativas, provenientes de aplicaciones móviles médicas o relacionadas con la salud, generadas por diferentes dispositivos portátiles, además de los mensajes de las redes sociales generales o específicas de salud o los metadatos (datos relacionados con la generación de otros datos, como es el caso de la geolocalización de los datos que genera un dispositivo).

En resumen, la actividad asistencial genera una enorme cantidad de información, de la que gran parte no está estructurada, por lo que sin un desarrollo tecnológico apropiado difícilmente se puede aprovechar para su tratamiento a gran escala.

4. Oportunidades del *Big Data* sanitario para las organizaciones sanitarias

El entorno sanitario es de gran complejidad. La mejora en las condiciones de vida de la población, los progresos en el tratamiento de las enfermedades

crónicas junto con el envejecimiento progresivo de la población han cambiado los patrones de las enfermedades. En este entorno cambiante, la irrupción de los sistemas de información sanitaria informatizados, incluyendo la aparición de la telemedicina o la historia clínica única entre los diferentes niveles asistenciales y sociosanitarios, ha permitido nuevos desarrollos y formas de atención impensables previamente.

La aplicación de los sistemas de inteligencia artificial a la organización del sistema sanitario puede aportar grandes ventajas potenciales. Se mencionan a continuación algunos de los posibles beneficios más destacados (14,19):

- **Sistemas de salud que aporten calidad en la asistencia**: las técnicas de *Big Data* permiten obtener datos a partir de la práctica clínica diaria para desarrollar modelos predictivos que se puedan incorporar como ayudas a la decisión tanto para profesionales como para gestores;

- Sistemas sanitarios que **fomenten la investigación**: la aplicación de tecnología *Big Data* permite construir modelos expertos capaces de autoaprendizaje que puedan generar conocimiento para la mejora de la salud, así como la posibilidad de realizar ensayos clínicos pragmáticos en condiciones de práctica clínica real;

- Sistemas sanitarios **seguros**: que incorporen herramientas de análisis de seguridad clínica, incluyendo prevención de errores y detección de incidentes, así como integrar los sistemas de farmacovigilancia (notificación automática de reacciones adversas de fármacos);

- Sistemas sanitarios **eficientes**: que sean capaces de comparar sus datos y resultados con otros sistemas de salud, que puedan medir la eficiencia de las innovaciones y detectar las intervenciones de escaso valor, así como poder seleccionar el perfil de pacientes que más se van a beneficiar de determinadas actuaciones asistenciales;

- Salud **centrada en los ciudadanos**: estas tecnologías pueden favorecer la progresiva incorporación de los ciudadanos a la toma de decisiones en salud, así como responder a la exigencia de transparencia en las administraciones en sus relaciones con los ciudadanos (14); permite incorporar los datos de sistemas de monitorización continua de múltiples variables de los usuarios para mejorar los resultados de salud, desarrollar apps móviles para la mejora de la

asistencia o la investigación, o incluso detectar desigualdades en el manejo de pacientes, o centrar las intervenciones en los colectivos más desfavorecidos;

- Sistemas con **orientación a la salud pública**: mediante el cruce de datos poblacionales de múltiples fuentes (datos socioeconómicos; evaluación de intervenciones poblacionales, detección precoz de epidemias y riesgos para la salud) con los datos de la historia clínica electrónica para aumentar el conocimiento en el ámbito de la salud pública;

- Sistemas que favorecen el **desarrollo de los profesionales**: facilitando la innovación y la incorporación del conocimiento a la práctica clínica mediante la difusión por la organización sanitaria y la formación de los profesionales; evitando tareas repetitivas de escaso valor que permitan a los profesionales dedicarse a los aspectos más personales de la asistencia (20).

5. Oportunidades del *Big Data* Sanitario en medicina personalizada

Además de la aplicación a la mejora del sistema sanitario en su conjunto, estas técnicas se aplican también a los modelos personalizados de medicina. La medicina personalizada o de precisión, consiste en la adaptación del tratamiento médico a las características individuales de cada paciente y de su enfermedad, como consecuencia de la integración de diferentes fuentes de datos a los modelos de enfermedad (21). De este modo, las posibles aplicaciones más destacadas de las tecnologías *Big Data* en este ámbito serían (19):

- Modelos **más completos de enfermedad**, desde el nacimiento hasta la muerte y desde la molécula a la sociedad, que incluyan los datos de diferentes fuentes y no únicamente de la historia clínica;

- Descubrimiento de **procesos biológicos fundamentales**, cruzando secuencias exómicas (regiones de los genes que codifican las proteínas) con los datos longitudinales de las historias clínicas;

- Desarrollo de **nuevas asociaciones** patológicas o terapéuticas analizando datos a gran escala de individuos que desarrollan patologías o cruzando información de la efectividad y eficiencia de los diferentes tratamientos;

- Descubrimiento de **nuevos mecanismos y diferentes subtipos de enfermedad** relevantes para el tratamiento, por ejemplo, variantes de tumores que responden de forma distinta a los diferentes tratamientos;

- Desarrollo de nuevas **dianas farmacológicas** o descubrimiento de nuevas indicaciones para fármacos ya existentes, acortando los procesos de desarrollo de nuevos fármacos;

- **Implantación de la medicina de precisión**, integrando el genoma en la historia clínica electrónica para elaborar modelos predictivos de enfermedad, utilizar los fármacos más eficaces y seguros para cada paciente, o incluso poner en marcha actividades de prevención del riesgo cardiovascular o de otro tipo más adecuadas al perfil genético (22);

- **Estimación personalizada** de riesgos y beneficios de las diferentes intervenciones sanitarias.

6. Riesgos y limitaciones de la tecnología *Big data*

Sin embargo, la aplicación de esta nueva tecnología no está exenta de amenazas. Como se ha mencionado, la utilización de tecnología *Big Data* supone unos riesgos para la privacidad que se pueden mitigar, pero no eliminar del todo, en vista de las posibilidades de reidentificación que ofrece el avance tecnológico.

Por este motivo, como se desarrolla a continuación, la legislación en materia de protección de datos ha evolucionado hacia un enfoque más proactivo desde la entrada en vigor del Reglamento Europeo (UE) 2016/679 general de protección de datos (en adelante, RGPD). Este enfoque está basado en los principios de la protección de datos: licitud, lealtad y transparencia del tratamiento (incluyendo el consentimiento y el derecho de información); la limitación de la finalidad; la minimización de los datos; la exactitud de los datos; la limitación del plazo de conservación y la integridad y confidencialidad de los datos. Por otra parte, el RGPD establece que el responsable del tratamiento será el responsable del cumplimiento de estos principios y capaz de demostrarlo (responsabilidad proactiva), lo que incluye la protección de datos desde el diseño y por defecto, la evaluación previa del impacto en los tratamientos que puedan suponer un alto riesgo para las libertades de

los sujetos o incluso, si es necesario, la consulta previa a la autoridad de protección de datos.

Son especialmente preocupantes las situaciones en las que una base de datos obtenida de forma lícita se combina posteriormente con otras bases de datos, de tal manera que se puedan reidentificar a los sujetos o se puedan utilizar estos datos para elaborar perfiles automatizados. A continuación, se mencionan algunas de las situaciones de riesgo que se pueden dar con el uso de estas tecnologías:

- Datos inicialmente anónimos por lo que no están sujetos a revisión ética o control legal que posteriormente se pueden reidentificar cruzándolos con otras bases de datos.

- Bases de datos obtenidas con un propósito lícito en las que se reutilizan los datos para usos secundarios no supervisados, tal y como podría ocurrir cuando la información obtenida para investigaciones previas o para la asistencia se transfiera a terceros o se reutilice con otros fines sin mediar un nuevo consentimiento.

- Transmisión de información a países cuya legislación no garantiza un nivel adecuado de protección de datos o a empresas con intereses comerciales sin el consentimiento de los sujetos.

- Generación de perfiles de riesgo de padecer enfermedades, determinadas condiciones o la puesta en marcha de sistemas de monitorización de conducta humana, lo que se puede realizar incluso con datos anónimos, exponiendo a los sujetos a situaciones de discriminación.

- Posibilidad de estigmatizar poblaciones vulnerables o mantener o incrementar desigualdades sociales, incluso en estudios con datos anonimizados.

- Considerar los datos disponibles en redes sociales como públicos, sin tener en cuenta la finalidad para la cual se hicieron públicos, utilizándolos para otros usos no lícitos o sin autorización.

- Conflictos en la legislación aplicable cuando la información se deposita en los entornos en línea, que pueden estar ubicados en terceros países con legislaciones que garantizan un menor nivel de protección de lo establecido en el RGPD.

- Propiedad de los datos depositados en redes sociales, en los que se autorizan unas condiciones de uso de los datos sin prestar atención a los términos por falta de una cultura de privacidad de los usuarios, teniendo en cuenta que dicha autorización se plantea siempre como un requisito obligatorio para acceder al servicio.

- Movimientos a favor de la transparencia de la información, que proponen que toda la información pertinente debe estar a disposición del público, incluyendo la exigencia de los editores de las publicaciones científicas de hacer disponibles las bases de datos originales de los estudios como medida para prevenir el fraude científico (23).

- Falta de formación, tanto de investigadores como de los miembros de los Comités de Ética de la Investigación, sobre las tecnologías de *Big data* y sus implicaciones éticas y legales.

Otra posible fuente de conflictos surge por el aprovechamiento comercial de los datos, dado que los grandes sistemas de bases de datos de salud pertenecen en su mayor parte a los sistemas públicos, mientras que la tecnología *Big Data* es propiedad generalmente de empresas privadas. Este hecho puede originar problemas éticos, legales e incluso políticos, cuando la cesión de datos de la Administración puede resultar en beneficios económicos a terceros.

Una limitación de los sistemas predictivos es que pueden ser útiles para el nivel de organización sanitaria, pero su utilización en pacientes individuales todavía no está contrastada respecto a la referencia, que es el juicio clínico de un profesional sanitario. Teniendo en cuenta que estas tecnologías se basan en predicciones a partir del procesamiento de datos retrospectivos, es lógico concluir que presentan limitaciones intrínsecas cuando se enfrentan a situaciones cambiantes o novedosas (11).

Otro riesgo que han señalado algunos autores es la probabilidad de que las aplicaciones de inteligencia artificial puedan poner en riesgo las interacciones personales que se dan en la asistencia entre facultativos y pacientes, influyendo desfavorablemente en las experiencias de ambos grupos. Estas amenazas, traducidas en desempleo médico y pérdida de habilidades clínicas, parecen exageradas. Del mismo modo que la toma automatizada de la tensión arterial o el recuento celular automatizado en el laboratorio han liberado a los clínicos de tareas repetitivas, la incorporación de la inteligencia artificial podría volver a dar sentido a la práctica de la medicina al tiempo

que se consiguen nuevos niveles de eficiencia y precisión. Los médicos deben guiar, supervisar y monitorizar, de una forma proactiva, la incorporación de la inteligencia artificial como un complemento en el cuidado del paciente (20,24).

7. Retos futuros del *Big Data* en la práctica clínica

La aplicación de técnicas de *Big Data* en el sector sanitario se enfrenta a algunos retos tecnológicos como los que se mencionan a continuación (2):

- Integrar la información de las diferentes fuentes disponibles (sanitario, socioeconómico, genómica y proteómica, imagen, redes sociales, sensores, aplicaciones móviles,…);
- Documentar la información de manera digital sin que requiera un esfuerzo añadido a los profesionales de la salud (mediante sistemas de codificación automática y de extracción de información a partir de texto libre);
- Analizar y procesar los datos no estructurados de salud (imagen, texto);
- Disponer de sistemas de almacenamiento físico de datos que puedan albergar una cantidad ingente de información;
- Disponer de medios técnicos y legales para compartir e intercambiar datos;
- Disponer de sistemas para asegurar la calidad de los datos (especialmente cuando se toman decisiones relevantes a partir de los resultados);
- Disponer de sistemas que aseguren la confidencialidad de los datos.

8. Experiencias de *Big Data* con grandes bases de datos sanitarios

Algunas de las experiencias infructuosas en el pasado con *Big Data* sanitario pueden servir como motivo de reflexión sobre las implicaciones éticas de estos proyectos.

El proyecto care.data fue promovido por el Servicio Nacional de Salud de Inglaterra (National Health Service England) en enero 2014 para utilizar los datos de las historias clínicas electrónicas de Atención Primaria con fines de investigación biomédica. Antes de su puesta en marcha se enviaron un total de 22 millones de folletos para informar a la población general del alcance del proyecto (25), a partir de los cuales se recibieron más de un millón de solicitudes de rechazo a la utilización de datos por la investigación. Posteriormente trascendió a los medios de comunicación que no se había respetado la opinión de los usuarios que se habían negado al tratamiento de sus datos (26). El proyecto se canceló en julio 2016 por la recomendación de la Autoridad de Protección de Datos de Salud Británica de establecer un modelo claro de oposición al tratamiento que abarcase diferentes opciones de retirada del consentimiento (27).

Una experiencia similar fue el proyecto VISC+ (Más valor a la información de salud en Cataluña) promovido por la Agencia de Calidad y Evaluación Sanitaria de Cataluña. Este proyecto consistía en contratar a una empresa privada para que desarrollase una plataforma para ceder los datos anonimizados del sistema sanitario público catalán, tanto para realizar proyectos de investigación como para otros fines con ánimo de lucro relacionados con las empresas farmacéuticas o biotecnológicas. Los diferentes informes que se elaboraron sobre los problemas éticos que planteaba este proyecto coincidieron en la preocupación suscitada por las posibles vulneraciones de los derechos de los ciudadanos y la falta de transparencia y debate público informado del proyecto (28). Finalmente, debido a la contestación pública y política, se desestimó el proyecto antes de su adjudicación (29).

El proyecto VISC+ ha sido sustituido por el programa PADRIS (Programa de Analítica de Datos para la Investigación e Innovación en Salud), gestionado exclusivamente por entidades públicas. Los datos anonimizados del PADRIS se suministrarán únicamente a los centros de investigación acreditados, públicos o sin ánimo de lucro, mediante una solicitud que incluya el protocolo de investigación y la aprobación previa por un Comité de Ética de la Investigación (CEI) (30). Aunque se prioriza la investigación independiente con financiación pública, no se impide el acceso a la investigación con financiación privada o mediante fórmulas de mecenazgo (31).

Otros proyectos de *Big Data* sanitaria son el proyecto CALIBER, plataforma promovida por el Servicio Nacional de Salud de Inglaterra, que ofrece variables "listas para la investigación" extraídas de diferentes bases de datos clínicas interrelacionadas. Esta plataforma incluye datos clínicos de atención primaria y

especializada sobre diagnósticos, constantes clínicas, resultados de laboratorio, prescripción farmacológica, vacunaciones, además de causas de fallecimiento y datos de deprivación social. Esta base de datos incluye información de 10 millones de personas con un seguimiento total de 400 millones de años-paciente. Las solicitudes de proyectos de investigación, que deben ser aprobadas por un Comité asesor científico independiente, tienen que acompañarse de la memoria del proyecto, así como del curriculum del investigador (32).

Las historias clínicas electrónicas de los Servicios Autonómicos de Salud son grandes repositorios de información que incluyen los datos de atención primaria y especializada, prescripción farmacéutica, resultados de laboratorio e información sociodemográfiica. Sin embargo, aún están pendientes de desarrollo las aplicaciones informáticas que permitan aprovechar esta información. Un ejemplo es BIFAP (Base de datos para la investigación fármaco-epidemiológica en Atención Primaria), gestionada por la Agencia Española del Medicamento y Productos Sanitarios con la colaboración de 9 Comunidades Autónomas, a la que aportan sus datos 6.800 médicos de familia y pediatras con más de 9 millones de historias clínicas anonimizadas (33).

Otros ejemplos de aplicación del *Big Data* sanitario son los sistemas comerciales que analizan los datos sanitarios a partir de la información ya disponible. IBM ha desarrollado la herramienta Watson Health, un sistema de inteligencia artificial aplicable al diagnóstico y tratamiento de enfermedades, a la gestión de servicios sanitarios, al desarrollo de nuevos fármacos o a la selección de participantes en ensayos clínicos (34). Una iniciativa similar es la propuesta por Savana, empresa española que ofrece unos módulos de Consulta (guías clínicas con datos en tiempo real); Research (extracción de variables automáticas para la investigación); Manager (descripción de patrones de consumo de recursos); Predict (herramienta de predicción de resultados) o EHRead (extractor de información clínica a partir de la historia clínica en castellano) (35). Otras herramientas están dedicadas exclusivamente a la investigación, como el Researchkit de Apple, que permite interactuar con los participantes en un proyecto de investigación, tanto para el reclutamiento como para la recogida de datos de forma automática o autorreferida por el participante (36).

9. Aplicación de la tecnología *Big Data* a la investigación clínica

Los sistemas de *Big Data* tienen la posibilidad de cambiar tanto la asistencia como la forma en la que se genera el conocimiento en que se basa la práctica clínica.

El modelo tradicional de investigación parte de una hipótesis que se intenta confirmar diseñando un experimento, incorporando posteriormente a la asistencia aquellas intervenciones que han demostrado su efectividad. El nuevo paradigma de la investigación biomédica, a partir de la implantación de tecnología *Big Data*, es la generación de hipótesis a partir de los datos obtenidos en la práctica clínica, que posteriormente se deben confirmar mediante una investigación (37).

La aplicación de la tecnología *Big Data* en la investigación biomédica permite realizar de forma relativamente sencilla estudios que hasta hace poco tiempo hubieran sido implanteables. De este modo, la disponibilidad de datos masivos procedentes de la asistencia sanitaria simplifica la realización de estudios observacionales, tanto retrospectivos como prospectivos. Son estudios en los que la información no se recoge con motivos de investigación, sino que se obtiene de la práctica clínica diaria (datos de la vida real o real world data) (16,38).

Como ejemplos de posibles diseños de estudios utilizando esta tecnología se pueden citar los siguientes:

- Estudios de cohortes prospectivas con seguimiento naturalístico a través de los datos del sistema de información sanitario, recogidos originalmente para la asistencia.

- Estudios de cohortes retrospectivas, seleccionando pacientes a partir una característica sucedida en el pasado y realizando el seguimiento desde ese momento hasta la actualidad.

- Estudios de casos y controles anidados en cohortes.

- **Ensayos clínicos pragmáticos** (aleatorizados), con seguimiento naturalístico (39). Este tipo de ensayos clínicos prometen ser uno de los avances con mayor capacidad de transformar la investigación clínica, cuyas ventajas más importantes serían las siguientes (40):

- Permite reclutar pacientes excluidos habitualmente de los ensayos clínicos (por ejemplo, grandes comorbilidades, enfermedad renal crónica avanzada o mujeres en edad fértil).

- Permite analizar variables de resultados duras (fallecimiento, entrada en diálisis), que con otros diseños de ensayos clínicos necesitan un

número elevado de pacientes seguidos durante mucho tiempo, lo que encarece extraordinariamente la investigación.

- Aumenta la eficiencia de los estudios buscando variables de resultado diferentes o seleccionando pacientes según características que hagan que los resultados sean más probables.

- Permite sistemas de ayuda a la selección de participantes utilizando algoritmos de análisis de lenguaje natural a partir de los evolutivos en texto libre de las historias clínicas electrónicas.

- Ofrece datos de efectividad en la práctica real, con información de los riesgos y beneficios a largo plazo de las intervenciones.

- Permite aportar datos en situaciones en las que no es posible realizar un ensayo clínico convencional, por no ser ético o impracticable.

- **Estudios exploratorios de relaciones entre datos** (data mining, data driven). Los nuevos modelos de investigación basada en datos parten de una hipótesis, pero en vez de diseñar un experimento para confirmarla, los investigadores analizan los datos disponibles y entonces diseñan experimentos o incluso utilizan datos adicionales para validar la hipótesis planteada. Los modelos guiados por datos (data driven) dan un paso adicional analizando los datos existentes sin una hipótesis fijada, este análisis genera una hipótesis que luego se confirma con el análisis de nuevos datos (38).

- **Estudios que utilizan técnicas de inteligencia artificial** (machine learning, redes neuronales), que constituyen los avances más significativos incorporados a la investigación. En estos estudios se procesan grandes cantidades de datos para entrenar un modelo de inteligencia artificial, que se utiliza para evaluar nuevos datos y ayudar a la toma de decisiones. Algunas de las herramientas más avanzadas de inteligencia artificial, tales como las redes neuronales profundas, no requieren una comprensión del mecanismo subyacente del modelo para lograr resultados predictivos increíblemente precisos. Este enfoque podría ser una herramienta valiosa para explorar datos cruzados de diferentes fuentes y apoyar decisiones clínicas, incluso cuando muchas interconexiones y relaciones entre estos datos son todavía desconocidas o ausentes (8,10,38).

Estas técnicas de inteligencia artificial son de algún modo contradictorias con el principio de minimización de datos que marca la legislación de protección de datos, dado que cuando se utilizan estas técnicas no se conocen a priori las variables que pueden aportar valor a los modelos predictivos.

En resumen, los estudios que utilizan la tecnología *Big Data* pueden ser de gran utilidad, tanto para mejorar los diseños de la investigación como para facilitar la realización de estudios en aspectos tales como la selección de participantes o el seguimiento electrónico.

10. Limitaciones de la investigación con *Big Data*

Sin embargo, la investigación con "datos de la vida real" tiene algunas limitaciones intrínsecas.

En primer lugar, todos los estudios observacionales incluyen sesgos difíciles de controlar ante la falta de aleatorización. Estos sesgos se pueden controlar con los ensayos clínicos pragmáticos aleatorizados, en los que la intervención se asigna al azar pero el seguimiento se hace en condiciones de práctica clínica real.

Una de las limitaciones principales de la investigación observacional es la dificultad de establecer relaciones de causalidad. En este tipo de investigaciones no se puede tener la certeza de que una asociación sea debida a una relación causa-efecto o por el contrario, a algún factor de confusión relacionado simultáneamente con las dos variables estudiadas, aunque se intente hacer un ajuste por las variables que el investigador considere más significativas (41). Otra causa importante de confusión es el sesgo de observación, por el cual a los pacientes sometidos a un seguimiento más intenso por su comorbilidad o por estar en tratamiento con un fármaco se les detecta más efectos secundarios que a una población control (39). En los estudios observacionales con seguimiento también puede aparecer el sesgo de selección, en el que los pacientes prevalentes de una condición, o los que ya están recibiendo un tratamiento, se comportan de forma diferente a aquellos en los que se acaba de hacer el diagnóstico o en los que se comienza el tratamiento, por lo que estos estudios deberían ajustar el resultado para los casos prevalentes e incidentes (42).

Otra limitación de los estudios observacionales es que los acontecimientos que definen el resultado estudiado se recogen a partir de la codificación de los

diagnósticos y procedimientos de los episodios asistenciales, por lo que dependen de la exhaustividad de esta codificación, que suele ser adecuada para los diagnósticos principales, pero puede ser menor para algunas condiciones crónicas coexistentes (hipertensión arterial, diabetes o tabaquismo) o para los diagnósticos que no están directamente relacionados con el motivo del ingreso. Por otra parte, en los estudios observacionales multicéntricos, puede haber diferencias de criterio en la codificación en los diferentes centros, lo que introduce sesgos sobre las variables de resultado (43).

Algunos autores han llamado la atención sobre los sesgos potenciales inherentes a los estudios con técnicas de inteligencia artificial, incluyendo la posibilidad de aumentar las desigualdades sociales (24). Algunas propuestas para reducir los errores en los algoritmos de aprendizaje de máquina serían la prevención de la confianza excesiva en la automatización, prevenir los sesgos en los datos que alimentan los algoritmos y tener en cuenta que los algoritmos pueden descubrir relaciones estadísticamente significativas, pero sin significación clínica. Se debería prestar atención a los datos que se utilizan para ajustar los algoritmos de inteligencia artificial, para saber qué datos y qué pacientes están ausentes y evitar así que las disparidades existentes en la asistencia aumenten por una confianza irreflexiva o excesiva en la computación (13).

Con el fin de mejorar la publicación de los estudios observacionales realizados a partir de los datos obtenidos de la historia clínica, se han publicado las guías RECORD (REporting of studies Conducted using Observational Routinely-collected health Data statement), que incluyen un listado de comprobación con los apartados que deberían incluirse en este tipo de publicaciones, para que se pueda valorar la validez interna y externa de los resultados (44). Estas guías son una adaptación de las recomendaciones previas STROBE (Strengthening the Reporting of OBservational studies in Epidemiology), dirigidas a la publicación de estudios observaciones en epidemiología (45).

Como conclusión, los estudios con datos de la vida real no sustituyen los datos de seguridad y eficacia obtenidos en los ensayos clínicos aleatorizados, pero sí que pueden contribuir a aumentar su validez externa.

11. Principios éticos en la investigación con *Big Data*

La irrupción de estas nuevas tecnologías ha supuesto que algunos autores se planteen si la ética de la investigación está obsoleta en la época del *Big*

Data (46). Sin embargo, aunque su aplicación deba adaptarse a esta nueva tecnología, se puede afirmar que los principios de la bioética, establecidos en el informe Belmont y desarrollados posteriormente en las diferentes pautas éticas internacionales sobre investigación biomédica, siguen siendo igualmente aplicables a estos estudios, incluyendo el respecto a la dignidad, autonomía, privacidad y confidencialidad de los participantes en una investigación (47,48,49,50,51). De este modo, las dimensiones éticas relevantes implicadas en este tipo de estudios son las siguientes (48):

Respeto por las personas: cualquier iniciativa que incluya el uso de datos tiene que considerar tanto los intereses privados como los públicos. Se debe permitir a los interesados expresar sus preferencias e informarles sobre la utilización de sus datos.

Respeto por los derechos humanos: los términos de cualquier uso de datos deberían respetar los derechos básicos, tales como la protección de la vida privada o familiar. Esto incluye establecer limitaciones a los gobiernos a interferir con la privacidad de los ciudadanos por motivos de interés público.

Participación e inclusión de los interesados: la utilización de datos debe tener en cuenta los deseos de los ciudadanos y, en lo posible, hacer participar a las personas y las comunidades a las que pertenecen en las decisiones acerca de sus datos.

Responsabilidad y rendición de cuentas: la utilización de datos debería rendir cuentas de forma pública mediante procedimientos legales, penales y políticos, además de rendir cuentas socialmente mediante el compromiso periódico de recoger las expectativas de la población sobre la utilización de sus datos. Las iniciativas que utilizan datos deben informar a los afectados de los fines del tratamiento, incluyendo información transparente sobre las posibles vulneraciones de la confidencialidad y cualquier desviación con la gobernanza establecida (48,50).

En este sentido, las iniciativas de utilización de *Big Data* sanitario deberían contar con el compromiso de la comunidad que aporta sus datos para contribuir a la mejora del sistema sanitario, a cambio del compromiso de los investigadores de que los datos estarán protegidos de revelaciones indebidas. Por este motivo, es imprescindible poner en marcha sistemas de gobernanza del *Big Data*, tanto para los responsables de los datos como para los encargados del tratamiento. Se debe elevar la exigencia a los profesionales

que manejan datos mediante políticas de acceso y privacidad que incluyan consecuencias rápidas y graves para el mal uso o la revelación de datos (52).

Teniendo en cuenta los beneficios esperables de la utilización de datos masivos, los sistemas de gobernanza de las bases de datos deben basarse preferentemente en los beneficios que puede aportar la investigación a la sociedad, sin olvidar los posibles perjuicios que pueda causar.

El cumplimiento de estos principios debería reflejarse en la gobernanza de datos que debería recoger al menos los siguientes aspectos clave (48):

- **Las disposiciones para el almacenamiento de datos** (dónde se custodian, con qué medidas de seguridad, por cuánto tiempo).

- **El acceso o transferencia de los datos** (si se hacen públicos, si se permite un acceso o transferencia controlados o únicamente se suministran datos indirectos).

- **El papel del consentimiento o de otras formas de autorización** (si se solicita consentimiento explícito, implícito dando opción a la no participación o con garantías adicionales como la autorización por comités u otros organismos).

- **Los usuarios autorizados** (incluyendo investigadores académicos, usuarios con intereses comerciales y cómo éstos demuestran (o no) que sus fines tienen un interés público).

Estos principios son similares a los recogidos en el RGPD, aprobado por la Unión Europea como respuesta a los nuevos retos para la protección de datos personales que plantean los avances tecnológicos.

Ya se han descrito precedentes de problemas éticos con el empleo de tecnología *Big Data* en investigación, como muestra de que las precauciones que suscita el uso de esta tecnología no son meramente teóricas. Un ejemplo ilustrativo es la controversia generada por la publicación del resultado de un experimento diseñado con el objetivo de demostrar que es posible producir un contagio emocional masivo sin comunicación directa con los usuarios (53). En este experimento se seleccionaron de forma aleatoria 689.000 usuarios de Facebook, en los que se filtraron las noticias positivas y negativas que recibían en comparación con un grupo control, demostrando que al reducir las noticias positivas, las personas eran menos propensas a

escribir mensajes positivos y viceversa. Los mensajes se calificaban como positivos o negativos mediante un algoritmo automático de análisis del lenguaje, de tal modo que los investigadores no tuvieron acceso al texto de los mensajes. Los investigadores no solicitaron el consentimiento de los usuarios ni se les advirtió de que estaban participando en una investigación, alegando que "el estudio era conforme con la política de utilización de datos de Facebook, aprobada por todos los usuarios antes de abrir una cuenta de Facebook, constituyendo esta aprobación el consentimiento informado para esta investigación" (53).

En una editorial posterior de la misma publicación se expresaron las dudas y la preocupación surgida sobre el respeto a los principios de consentimiento informado y a la opción de rechazar la participación a los implicados, como garantía de las mejores prácticas posibles en investigación. La editorial remarcaba también que el estudio no fue aprobado por un CEI debido a que la investigación fue realizada por Facebook con fines privados (54).

Similares preocupaciones se han suscitado con otros estudios, en los que se han puesto a disposición de la comunidad investigadora información tan sensible como la base de datos de los usuarios de un sitio web de contactos, en la que los usuarios podían identificarse fácilmente, con el argumento de que la información que se proporciona en estas páginas es pública (46).

12. Control ético y legal de los proyectos *Big Data*

Teniendo en cuenta los posibles riesgos mencionados previamente, el control ético y legal de los proyectos de investigación que utilizan tecnologías *Big Data* ha sido un motivo de preocupación para los Comités de Ética de la investigación y los propios investigadores.

La entrada en vigor del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) ha cambiado el panorama legislativo de la utilización de datos relacionados con la salud en investigación, tanto para la utilización de datos identificados, seudonimizados e incluso anonimizados.

El consentimiento para utilizar los datos para una investigación se obtiene generalmente en el momento de recabarlos, teniendo en cuenta que la LOPD-GDD permite que este consentimiento para investigación sea con fines amplios. Cuando se plantea reutilizar los datos obtenidos previamente surgen

dos problemas fundamentales: determinar si el consentimiento otorgado aún refleja los deseos del sujeto y si los nuevos usos propuestos se consideran incluidos en el consentimiento original, por este motivo la LODP-GDD exige que la reutilización de datos de investigaciones previas deba estar supervisada por un CEI cuando la recogida de datos sea posterior a la entrada en vigor de la LOPD-GDD.

Hasta la entrada en vigor de esta Ley, la utilización de datos anonimizados carecía de regulación legal, al no considerarse datos de carácter personal. Sin embargo, la LOPD-GDD establece, de acuerdo con el RGPD, que los estudios con datos relacionados con la salud tengan una evaluación previa del impacto que incluya, "*de modo específico, los riesgos de reidentificación vinculados a la anonimización y seudonimización de los datos*". La Ley también prevé que el uso de datos personales seudonimizados con fines de investigación biomédica deberá ser sometido al informe previo de un CEI. Este dictamen también sería aplicable a las investigaciones que utilicen datos anonimizados, tal como se desprende del enunciado de la LOPD-GDD, que exige la incorporación de un delegado de protección de datos o un experto en protección de datos a la composición de los comités de ética de la investigación "*cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados*".

La LOPD-GDD establece también el régimen sancionador en las infracciones a la protección de datos, considerando como infracciones muy graves tanto la reversión deliberada de un procedimiento de anonimización, a fin de permitir la reidentificación de los afectados, como la utilización de datos disponibles para otros fines, no autorizados o lícitos, o la transferencia internacional de datos cuando no concurran las garantías, requisitos o excepciones establecidos en el RGPD.

13. La utilización de datos anonimizados

Tal como se ha comentado, el paradigma de la anonimización de los datos como garantía absoluta de privacidad tiene actualmente serias limitaciones, dado que las posibilidades de reidentificación que ofrece la informática son cada vez mayores, dependiendo de la información adicional disponible (tanto en el momento actual como en un futuro) y del esfuerzo que se dedique.

La única forma de garantizar la imposibilidad de reidentificar a un individuo es recodificar y agrupar las variables que podrían identificar eventualmente a un individuo, tales como la fecha de nacimiento, el lugar de residencia o la fecha de un ingreso hospitalario (4,55). Cuando se llevan a cabo estas técnicas de anonimización, siempre se distorsiona y pierde parte de la información (el llamado diferencial de privacidad), de tal manera que deberá llegarse a un compromiso entre los fines del tratamiento y las amenazas para la privacidad (55). Una garantía adicional para evitar la reidentificación es que las personas implicadas en el tratamiento de la información personal anonimizada no tengan acceso a los datos personales no anonimizados o que no conozcan los mecanismos y claves de anonimización utilizados (55).

El RGPD exige que se garantice el respeto al principio de minimización de datos personales en el tratamiento de datos con fines de investigación biomédica. El RGPD especifica que se pongan en marcha medidas como la seudonimización, siempre que la investigación se pueda realizar de esta forma, pero que si la investigación se puede realizar con datos anonimizados, deberá llevarse a cabo de ese modo.

La LOPD-GDD ha previsto la utilización de datos seudonimizados o anonimizados para investigación sin el consentimiento del sujeto, siempre que se pongan en marcha las medidas técnicas y organizativas suficientes para prevenir la reidentificación y que los investigadores no tengan acceso a los datos identificativos. Estas medidas incluyen una evaluación del impacto en la protección de datos cuando sea necesario, así como desarrollar un enfoque proactivo en la protección de datos, incluyendo las medidas de protección por defecto y desde el diseño de la investigación. Como garantía adicional, la LOPD-GDD exige que estos proyectos cuenten con el informe previro del comité de ética de la investigación.

En resumen, aunque la entrada en vigor de la LOPD-GDD ha supuesto un gran avance en la regulación de la investigación con datos relacionados con la salud, incluyendo el *Big data* sanitario, todavía existen dudas en la interpretación del texto legal, especialmente en cuanto al tratamiento de datos anonimizados. En ausencia de un desarrollo mediante Reglamento como la anterior LOPD, deberá esperarse la interpretación de los informes que emitan las Autoridades de protección de datos.

14. Conclusiones

- La utilización de la tecnología *Big data* en la práctica clínica puede aportar grandes beneficios para la atención sanitaria y la investigación clínica.

- Para conseguir estos objetivos es fundamental la integración de las diferentes fuentes de información.

- Es necesario garantizar el uso y la aplicación de la tecnología *Big data* en un marco ético y jurídico adecuado, tanto en asistencia como en investigación.

- La utilización de estas tecnologías puede suponer una fuerte amenaza para la privacidad, por lo que es esencial poner en marcha procedimientos de control de la información que sean adecuados, transparentes y seguros y que garanticen el máximo nivel de confidencialidad y el respeto a los derechos y libertades de las personas.

- El personal sanitario, los investigadores, los Comités de ética de la investigación y las autoridades sanitarias y de protección de datos tienen como deber compartido el compaginar de forma equilibrada la protección de datos con la investigación relevante y la práctica clínica.

- La reciente aprobación del RGPD y la LOPD-GDD ha incorporado la regulación del uso de datos a gran escala con fines asistenciales y de investigación, incluyendo los datos identificados, seudonimizados y anonimizados.

15. Bibliografía

1. Aced, E. / Heras, M.R. / Sáiz, C.A., *Código de buenas prácticas en protección de datos para proyectos Big Data,* Agencia Española de Protección de Datos [En línea, consultado el 28/02/2019]. Disponible en: www.agpd.es.
2. Menasalvas, E. / Gonzalo-Martín, C. / Rodríguez-González, A., "Big Data en salud: retos y oportunidades", *Economía Industrial*, Vol. 405, 2017, pp. 87-97.
3. European Commission, *eHealth Task Force Report - Redesigning health in Europe for 2020,* Luxembourg, 2012.

4. Article 29 Data Protection Working Party, *Opinion 05/2014 on anonymisation techniques*, 2014 [En línea, consultado el 28/02/2019]. Disponible en: https://ec.europa.eu/justice/article-29/documentation/
5. Sweeney, L., *Simple demographics often identify people uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, 2000.
6. Goodfellow, I. / Bengio, Y. / Courville, A., *Deep Learning*. In. Cambridge, Mass: MIT Press; 2016, pp. 1-26 [En línea, consultado el 28/02/2019] Disponible en: http://www.deeplearningbook.org/contents/intro.html
7. Naylor, CD., "On the Prospects for a (Deep) Learning Health Care System", *JAMA*, Núm. 11, Vol. 320, 2018, pp. 1099-1100.
8. Chartrand G. / Cheng, P.M. / Vorontsov, E. / Drozdal, MTS. / Pal, C.J. / Kadoury, S. *et ál*. "Deep Learning: A Primer for Radiologists", *RadioGraphics*, Vol. 37, 2017, pp. 2113-31.
9. Hinton, G., "Deep Learning–A Technology with the potential to transform health care", *JAMA,* Núm. 11, Vol. 320, 2018, pp. 1101-2.
10. Beam, A.L. / Kohane, I.S., "Big Data and Machine Learning in Health Care", *JAMA,* Núm. 13, Vol. 319, 2018, pp. 1317-8.
11. Stead, WW., "Clinical implications and challenges of artificial intelligence and deep learning", *JAMA*, Vol. 320, 2018, pp. 1107-8.
12. Rajkomar A., "Scalable and accurate deep learning with electronic health records", *npj Digital Med*. Núm. 18, Vol. 1, 2018.
13. Gianfrancesco, M.A. / Tamang, S. / Yazdany J. / Schmajuk, G., "Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data", *JAMA Intern Med*., Núm. 11, Vol. 178, 2018, pp. 1544-47.
14. Murdoch, T.B. / Detsky A.S., "The Inevitable Application of Big Data to Health Care", *JAMA*, Núm. 13, Vol. 309, 2013, pp. 1351-2.
15. Clasificación Internacional de Enfermedades. Organización Panamericana de la Salud [En línea, consultado el 28/02/2019]. Disponible en: https://www.paho.org/hq/
16. García López JL. / Del LLano Señarís, J.E. / Del Diego Salas J. / Recalde Manrique, J.M., *Aportación de los "Real World Data" a la mejora de la práctica clínica y del consumo de recursos de los pacientes*, Fundación Gaspar Casal, 2014.
17. Comité de Ética del Instituto de Investigación de Enfermedades Raras, "Guías Éticas de Investigación en Biomedicina", 2009 [En línea, consultado el 29/02/2019]. Disponible en: http://publicaciones.isciii.es/
18. Universidad Politécnica de Madrid, *Big Data en Salud*, Informe de vigilancia tecnológica, 2015 [En línea, consultado el 28/02/2019]. Disponible en: https://fipse.es/sites/default/files/documentos/
19. Hemingway, H. / Asselbergs, F.W. / Danesh, J. / Dobson, R. / Maniadakis, N. / Maggioni, A. *et ál.,* "Big data from electronic health records for early and late translational cardiovascular research: challenges and potential", *European Heart Journal*, Núm. 16, Vol. 39, 2017, pp. 1481-95.
20. Verghese, A. / Shah, N.H. / Harrington, R.A., "What This Computer Needs Is a Physician Humanism and Artificial Intelligence", *JAMA*, Núm. 1, Vol. 319, 2018, pp. 19-20.

21. Sociedad Española de Oncología Médica, [En línea, consultado el 28/02/2019]. Disponible en: https://seom.org/informacion-sobre-el-cancer/ique-es-la-medicina-de-precision
22. Cabaleiro, T. / Prieto-Pérez, R. / Ochoa, D. / Abad-Santos, F., "Aplicación de la farmacogenómica y otras nuevas tecnologías al desarrollo de medicamentos", *Medicina Clínica*, Núm. 12, Vol. 140, 2013, pp. 558-63.
23. The Center for Scientific Integrity. Retraction Watch. [En línea, consultado el 28/02/2019]. Disponible en: https://retractionwatch.com
24. Israni, S.T. / Verghese, A., "Humanizing Artificial Intelligence", *JAMA*, Núm. 1, Vol. 321, 2019, pp. 29-30.
25. Nhs Choices, *National Health Service England. Better information means better care*, 2014 [En línea, consultado el 28/02/2019]. Disponible en: https://www.england.nhs.uk/wp-content/uploads/2014/01/cd-leaflet-01-14.pdf
26. Ramesh, R. "NHS disregards patient requests to opt out of sharing medical records", *The Guardian*. 22/01/2015.
27. Nhs England, *care.data NHS England*, 2016 [Consultado el 1/03/2019]. Disponible en: https://www.england.nhs.uk/2013/10/care-data/
28. Llácer, M.R. / Casado, M. / Buisan, L., *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública,* Dret OdBi, editor. Barcelona: Publicacions i Edicions de la Universitat de Barcelona, 2015.
29. Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS), Generalitat de Catalunya, 2016 [En línea, consultado el 28/02/2019]. Disponible en: http://aquas.gencat.cat/es/detall/detall-noticia/VISC_cancelacio_dialegCompetitiu.
30. Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS), *Programa de analítica de datos para la investigación y la innovación en salud (PADRIS)* [En línea, consultado 01/03/2019]. Disponible en: http://aquas.gencat.cat/es/ambits/analitica-dades/padris/index.html
31. Agència de Qualitat i Avaluació Sanitàries de Catalunya, Departament de Salut. Generalitat de Catalunya. rograma públic d'analítica de dades per a la recerca i la innovació en salut a Catalunya –PADRIS–. 2017 [En línea, consultado el 28/02/2019]. Disponible en: http://aquas.gencat.cat/web/.content/minisite/aquas/publicacions/2017 /Programa_analitica_dades_PADRIS_aquas2017.pdf .
32. Caliber. Ucl Institute Of Health Informatics. [En línea, consultado el 28/02/2019]. Disponible en: https://www.ucl.ac.uk/health-informatics/caliber.
33. Agencia Española del Medicamento y Productos Sanitarios. BIFAP. [En línea, consultado el 28/02/2019]. Disponible en: http://www.bifap.org/.
34. Ibm. Ibm Watson Health. [En línea, consultado el 28/02/2019]. Disponible en: https://www.ibm.com/watson/health/index-1.html.
35. Savana. [En línea, consultado el 28/02/2019]. Disponible en: https://savanamed.com/es/.
36. Apple. Researchkit. [En línea, consultado el 28/02/2019]. Disponible en: https://www.apple.com/es/researchkit/.

37. Embi, PJ. / Payne, PR., "Evidence Generating Medicine: Redefining the Research-Practice Relationship to Complete the Evidence Cycle", *Medical Care*, Núm. 8 (Supl 3)), Vol. 51, 2013, s87-91.
38. Zhu, L. / Zheng, W.J., "Informatics, Data Science, and Artificial Intelligence", *JAMA*, Núm. 11, Vol. 320, 2018, pp. 1103-4.
39. Mc Cord, K.A. / Salman, R.A. / Treweek, S. / Gardner, HSD. / Whiteley, W. / Ioannidis, JPA. *et ál.*, "Routinely collected data for randomized trials: promises, barriers, and implications", *Trials,* Núm. 29, Vol. 19, 2018.
40. Lauer, M.S. / D'Agostino, R.B., "The Randomized Registry Trial – The Next Disruptive Technology in Clinical Research", *NEJM,* Vol. 369, 2013, pp. 1579-81.
41. Lazarus, B. / Chen, Y. / Wilson, F.P. / Sang, Y. / Chang, A.R. / Coresh, J. *et ál*, "Proton Pump Inhibitor Use and Risk of Chronic Kidney Disease", *JAMA Intern Med*., Núm. 2, Vol. 176, 2016, pp. 238-46.
42. Danaei, G. / Tavakkoli, M. / Hernán, M.A., "Bias in Observational Studies of Prevalent Users: Lessons for Comparative Effectiveness Research From a Meta-Analysis of Statins", *Am J Epidemiol*, Núm. 4, Vol. 175, 2012, pp. 250–62.
43. Li, L. / Rothwell, P.M., "Biases in detection of apparent `weekend effect´ on outcome with administrative coding data: population based study of stroke", *BMJ*, Vol. 353, 2016, i2648.
44. Benchimol, E. I. / Smeeth, L. / Guttmann, A. / Harron, K. / Moher, D. / Peterson, I. / Sorensen, H.T. / Von Elm, E. / Langan, S.M., "Record Working Committee. The REporting of studies Conducted using Observational Routinely-collected health Data (RECORD) Statement", *PLoS Med*, Núm. 10, Vol. 12, 2015, e1001885.
45. Von Elm E. / Altman DG. / Egger, M. / Pocock, S.J. / Gotzsche, P.C. / Vanderbroucke, J.P. *et ál.* "The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies", *PLOS Medicine*, Núm. 10, Vol. 4, 2007, e296.
46. Leetaru, K., "Are Research Ethics Obsolete In The Era Of Big Data?", *Forbes*, 17 Junio, 2016.
47. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *Office for Human Research Protections. U.S. Department of Health and Human Services. The Belmont Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research*, 1979 [En línea, consultado el 28/02/2019]. Disponible en: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html
48. Nuffield Council on Bioethics, *The collection, linking and use of data in biomedical research and health care: ethical issues,* Londres, 2015 [En línea, consultado el 28/02/2019]. Disponible en: http://nuffieldbioethics.org/project/biological-health-data
49. Consejo de Organizaciones Internacionales de las Ciencias Médicas (CIOMS), *Pautas éticas internacionales para la investigación relacionada con la salud con seres humanos,* Ginebra, 2017.

50. Asociación Médica Mundial, *Declaración de la AMM sobre las Consideraciones Eticas de las Bases de Datos de Salud y los Biobancos*, 2017 [En línea, consultado el 28/02/2019]. Disponible en: https://www.wma.net/es
51. Asociación Médica Mundial, *Declaración de Helsinki. Principios éticos para las investigaciones médicas en seres humanos,* 2013 [En línea, consultado el 28/02/2019]. Disponible en: https://www.wma.net/es
52. European Economic and Social Committee, *The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context*, 2017.
53. Kramer, ADI. / Guillory, J.E. / Hancock, J.T., "Experimental evidence of massive-scale emotional contagion through social networks", PNAS, Núm. 24, Vol. 111, 2014, pp. 8788-9
54. Verma, I.M. Editor in Chief. Editorial Expression of Concern: Experimental evidence of massivescale emotional contagion through social networks. PNAS. 2014; 111(29): 10779
55. Agencia Española de Protección de Datos, *Orientaciones y garantías en los procedimientos de anonimización de datos personales,* 2016 [En línea, consultado el 28/02/2019]. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud*

Revision of the legal categories of the European regulation in the face of big data technology applied to health

Prof. Dr. iur. Dr. med. Carlos María Romeo-Casabona

Catedrático de Derecho Penal de la Universidad del País Vasco UPV/EHU

Investigador Principal del Grupo de Investigación Cátedra de Derecho y Genoma Humano de la Universidad del País Vasco UPV/EHU (Bilbao, España)

DOI: 10.14679/1134

Sumario / Summary: 1. Introducción. El nuevo marco jurídico europeo sobre protección de datos personales. 2. Implicaciones del *big data* para el régimen legal de los datos personales. 3. El dato relativo a la salud. Insuficiencias conceptuales. 4. La secuenciación masiva de genomas humanos: revisión del estatuto jurídico de los datos genéticos. 5. Revisión del estatuto jurídico sobre el tratamiento de los datos de salud. Respuestas a los nuevos riesgos. 5.1. Clasificación de las personas en grupos o subgrupos de acuerdo con sus perfiles personales. 5.2. Tendencia a tomar

* Artículo recibido el 24 de agosto de 2019 y aceptado para su publicación el 16 de septiembre de 2019.

El presente trabajo se realiza en el marco de la financiación del Gobierno Vasco a Grupos de Investigación del Sistema Universitario Vasco (IT 1066-16); y en el de la licencia sabática concedida por la UPV/EHU y forma parte del Proyecto de Investigación Bigdatlus (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos -*Big Data*-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

decisiones automatizadas de las personas. 5.3. La seudonimización como vía de protección de datos personales. 6. La reidentificación y los requisitos de cesión de datos. 6.1. El *big data* y los riesgos de reidentificación de los datos anonimizados o seudonimizados. 6.2. La prevención de la reidentificación. 7. Consideraciones finales. Algunas propuestas.

Resumen / Abstract: El nuevo RGPD dedica una mayor atención específica a los datos personales relativos a la salud, lo cual era estrictamente necesario. Además, se incluyen de forma explícita y por primera vez varias referencias a los datos genéticos en cuanto datos relativos a la salud, aunque separados de éstos. La posición actual de la UE y de los EM sobre el estatuto jurídico de los datos relativos a la salud ha cambiado sensiblemente, pues, aunque éstos conservan su condición de datos "sensibles", esto es, de datos que gozan de una protección jurídica especial, se ha decidido también facilitar el acceso a estos datos por parte de los diversos profesionales de la salud que tengan que prestar su actividad asistencial con el fin de ganar en eficacia y en rapidez respecto a dicho acceso. Mientras que en este supuesto se han querido primar los intereses del propio titular de los datos en relación con su salud, en el caso de la investigación relativa a la salud o biomédica con la eliminación o relajación de ciertos requisitos se ha dado preferencia al interés social que representa la misma frente al derecho individual a la protección de los datos personales, en la medida en que los resultados y avances científicos en el sector de la salud contribuyen al bienestar de la colectividad. Es obvio que otras disposiciones de carácter más general, que atienden también a situaciones nuevas o cambiantes, y por tanto a las necesidades jurídicas actuales, serán aplicables asimismo a los datos relativos a la salud; así, respecto al tratamiento masivo de datos y el flujo transnacional de datos, que han experimentado modificaciones relevantes con el nuevo marco legal europeo y, como es sabido, ambos supuestos son de extraordinario interés para los datos relativos a la salud. Coherentemente, la legislación interna de nuestro país sobre protección de datos personales ha sido objeto de revisión y de adaptación parlamentarias al RGPD mediante la promulgación de una nueva ley orgánica. En este artículo el autor estudia algunos conceptos y categorías jurídicas nuevos o revisados por la nueva regulación europea o que requieren un enfoque diferente, con el fin de delimitar su verdadero significado y alcance en la actualidad. Para este fin, tiene presente la nueva regulación estatal sobre protección de datos cuando resulta pertinente.

The new GDPR devotes more specific attention to personal data relating to health, which was strictly necessary. In addition, for the first time a number of references to genetic data are explicitly included as health-related data but separate from them. The current position of the EU and the MS on the legal status of health data has changed significantly, even though they retain their status as "sensitive" data, i.e. data enjoying special legal protection, it has also been decided to facilitate access to these data by the various health professionals who have to provide care in order to increase the efficiency and speed of such access. While in this case the interests of the data subject in relation to his/her health have been prioritised, in the case of health or biomedical research with the elimination or relaxation of certain requirements, preference has been given to the social interest which it represents over the individual right to the protection of personal data, insofar as scientific results and advances in the health sector contribute to the well-being of the community. It is obvious that

other provisions of a more general nature, which also deal with new or changing situations, and therefore with current legal needs, will also apply to data relating to health; thus, with regard to the massive processing of data and the transnational flow of data, which have undergone relevant modifications with the new European legal framework and, as is known, both assumptions are of extraordinary interest for data relating to health. Consistently, our country's internal legislation on the protection of personal data has been subject to parliamentary revision and adaptation to the GDPR through the enactment of a new fundamental law. In this paper the author studies some legal concepts and categories that are new or revised by the new European regulation or that require a different approach, in order to delimit their true meaning and scope at present. To this end, the author takes into account the new state regulation on data protection when it is relevant for that purpose.

Palabras clave / Keywords:

Reglamento General de Protección de Datos (RGPD) / Protección de datos / Datos de salud / Datos genéticos / Seudonimización.

General Data Protection Regulation (GDPR) / Data protection / Health data / Genetic data / Pseudonymization.

1. Introducción. El nuevo marco jurídico europeo sobre protección de datos personales

El vertiginoso desarrollo del tratamiento de los datos de carácter personal que se ha producido desde que la UE aprobara en 1995 la Directiva sobre protección de datos personales[1] condenó a la obsolescencia una buena parte de dicha normativa, que tan innovadora fuera hace más de dos décadas. El marco jurídico que se instauró con esta Directiva para el espacio europeo y para las relaciones de los Estados Miembros entre sí y con otros estados no miembros fue quedando muy angosto y llegó a ser insuficiente para hacer frente a tantas novedades tecnológicas y sociales relacionadas que se han ido produciendo, así como a la mayor complejidad que ha adquirido su tratamiento[2].

En el ámbito de los datos relativos a la salud esta rápida evolución ha sido más evidente si cabe. En efecto, tanto en la actividad asistencial, como en la epidemiología y en la investigación científica biomédica se ha comprobado la importancia que tiene el tratamiento de los datos relativos a la salud para

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

[2] Lo cual fue denunciado por los autores. V., en este sentido, Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, Troncoso Reigada, Antonio (Coord.), Ed. Thomson Reuters, Cizur Menor, España, *en prensa*.

poder realizar con éxito estas actividades, acrecentada por el apoyo con sistemas de inteligencia artificial y de procedimientos automatizados en general[3].

De ahí que el RGPD[4] dedique una mayor atención específica a los datos personales relativos a la salud, lo cual, por lo demás, era estrictamente necesario. Además, se incluyen de forma explícita y por primera vez varias referencias a los datos genéticos en cuanto datos relativos a la salud, aunque separados de éstos.

La posición actual de la UE y de los EM sobre el estatuto jurídico de los datos relativos a la salud ha cambiado notablemente, pues aunque éstos conservan su condición de datos "sensibles", esto es, de datos que gozan de una protección jurídica especial –reforzada–, se ha decidido también facilitar el acceso a estos datos por parte de los diversos profesionales de la salud que tengan que prestar su actividad asistencial con el fin de ganar en eficacia y en rapidez respecto a dicho acceso (p. ej., en situaciones de urgencia del interesado). Mientras que en este supuesto se han querido primar los intereses del propio titular de los datos en relación con su salud, en el caso de la investigación relativa a la salud o biomédica con la eliminación o relajación de ciertos requisitos (p. ej., el consentimiento del interesado) se ha dado preferencia al interés social que representa la misma frente al derecho individual a la protección de los datos personales, en la medida en que los resultados y avances científicos en el sector de la salud contribuyen al bienestar de la colectividad.

Es obvio que otras disposiciones de carácter más general, que atienden también a situaciones nuevas o cambiantes, y por tanto a las necesidades jurídicas actuales, serán aplicables asimismo a los datos relativos a la salud; así, respecto al tratamiento masivo de datos (*big data*) y el flujo transnacional de datos, que han experimentado modificaciones relevantes con el nuevo marco legal europeo y, como es sabido, ambos supuestos son de extraordinario interés para los datos relativos a la salud.

Coherentemente, la legislación interna de nuestro país y de algunos más, como Francia y Alemania, sobre protección de datos personales ha

---

[3] V. sobre este asunto con más detalle, Romeo Casabona, Carlos María / Lazcoz Moratinos, Guillermo, "Inteligencia artificial aplicada a la salud: ¿qué marco jurídico?", *E-salud y cambio del modelo sanitario*, Sánchez-Caro, Javier / Abellán, Fernando (Coords.), Fundación Merck Salud, Madrid, España, 2019 (en prensa).

[4] Reglamento General sobre la Protección de Datos Personales 2016/769, de 27 de abril de 2016.

sido objeto de revisión y de adaptación parlamentarias al RGPD mediante la promulgación de una nueva ley orgánica[5].

En este estudio vamos a ver algunos conceptos y categorías jurídicas nuevos o revisados por la nueva regulación europea o que requieren un enfoque diferente, con el fin de delimitar su verdadero significado y alcance en la actualidad. Para este objetivo tendremos también presente la nueva regulación estatal sobre protección de datos cuando ello sea pertinente.

2. Implicaciones del *big data* para el régimen legal de los datos personales

Con la expresión *big data* suele acotarse una variedad de tecnologías mediante las cuales puede ser tratada una cantidad masiva de datos de origen muy diverso relativos a una misma persona o a un número extenso de ellas[6]. Se trata, pues, de volúmenes muy elevados de datos.

El objetivo del tratamiento de estos datos es obtener de ellos ciertas utilidades, como puede ser, por ejemplo, conocer los patrones de comportamiento de los clientes o usuarios de una organización con el fin de orientar mejor las campañas publicitarias o de mercado dirigidas a ellos; o predecir tendencias y descubrir variables desconocidas incluso para los propios interesados relativas a personas, entidades o empresas que facilitan la innovación en los sectores más variados: económico, financiero, consumo, ocio e, indudablemente, salud, además de otros.

Los efectos del tratamiento de grandes volúmenes de datos son muy variados. Así, permite establecer relaciones entre datos muy diversos y obtener conclusiones que sería imposible o muy difícil de extraer a partir de cantidades de datos reducidas o más homogéneas. El cruce masivo de datos anónimos con otros personales (identificados o identificables: seudonimizados)[7] puede dar lugar a la identificación o a volver a identificar –reidentificar– al interesado. En el campo de la salud el tratamiento de datos masivos puede ayudar

---

[5] Ley Orgánica de Protección de Datos Personales y Garantías y Derechos Digitales (LOPDGDD) 2/2018, de 5 de diciembre.

[6] Sobre las características y potencialidades de los *big data* v. Delort, P., *Le big data*, Presses Universitaires de France, París, Francia, 2015, pp. 41 y ss.

[7] Pizzetti, F., *Privacy e il Diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, I*, G. Giappichelli Editore, Torino, Italia, 2016, pp. 190 y s.

a identificar numerosas enfermedades[8] y descubrir un creciente número de predisposiciones a desarrollar enfermedades cuya manifestación es incierta o revelar la condición de portador de enfermedades hereditarias, la tolerancia individual a ciertos tratamientos, principalmente con medicamentos, lo que es de especial interés para la Medicina Preventiva y para la Medicina Personalizada de Previsión, que serán los grandes y prioritarios objetivos y enfoques de la Medicina de los próximos años.

El *big data* comporta no sólo un cambio cuantitativo en el procesamiento de los datos (enormes cantidades de datos), sino sobre todo un cambio cualitativo, en cuanto que su tratamiento hace posible la obtención de información que aparentemente no está implícita en los datos recopilados o no puede derivarse o deducirse directamente de ellos. Esta apreciación a su vez sugiere varias novedades que son relevantes para la normativa relativa a la protección de datos:

i) El elevado riesgo de identificar o a volver a identificar –reidentificar– con relativa facilidad datos anónimos o que han sido anonimizados o seudonimizados, como pertenecientes a una persona determinada –o determinable–, estableciendo relaciones con datos masivos a través de las tecnologías del *big data* y de la llamada minería de datos[9].

ii) La disposición de información voluminosa sobre el paciente (p. ej., aumento de información sintomática o de carácter predictivo sobre predisposición a determinadas enfermedades). Este escenario requerirá decidir si se transmite al paciente toda la información obtenida, lo que puede plantear una posible responsabilidad por exceso de información, o seleccionar cuál le será comunicada y conforme a qué criterios (grado de probabilidad, gravedad de la enfermedad, existencia o no de tratamiento eficiente, etc.)[10].

iii) La toma de decisiones basadas exclusivamente en procesos de automatización o en perfiles obtenidos de los pacientes, sin perjuicio de su evidente utilidad, puede afectar a la autonomía del paciente, disminuyéndola o vaciándola de contenido.

---

8 Destaca la relevancia de esta posibilidad el cndo. 157 del RGPD.

9 Proceso que se vale de la estadística y de las ciencias de la computación dirigido al hallazgo de patrones en grupos de datos masivos.

10 V. Romeo Casabona, Carlos María / Lazcoz Moratinos, Guillermo, *Inteligencia artificial aplicada a la salud: ¿qué marco jurídico?*, *op. cit.*

iv) La tendencia al automatismo en la toma de decisiones cuando están basadas exclusivamente en propuestas algorítmicas del sistema de IA, que pueden anular la iniciativa y la independencia decisional del profesional, sustituyéndola, a veces siendo aceptada por aquél sin fundamentos suficientes.

v) El riesgo de que al clasificar o estratificar a los pacientes en grupos o subgrupos de acuerdo con los perfiles personales obtenidos de ellas con diversos criterios u objetivos, se tomen decisiones discriminatorias[11], estigmatizadoras o arbitrarias basadas exclusivamente en esos perfiles.

vi) La opacidad sobre los elementos esenciales y sobre el proceso por el que un sistema de IA ha llegado a una conclusión decisoria (indica su propuesta, pero no aporta información significativa sobre en qué elementos o factores causales se ha fundamentado aquélla), comporta el riesgo de que el profesional de la salud no pueda validar y confirmar o descartar razonadamente la propuesta del sistema al adoptar su propia decisión, lo que puede conducir a discutir su posible responsabilidad si se acredita que hubo algún error en el sistema o en el propio profesional que repercutiera en el empeoramiento del estado de salud del paciente.

vii) El aumento de prácticas discriminatorias o estigmatizadoras en diversos ámbitos, además del mencionado más arriba, las cuales están prohibidas por la comunidad internacional[12] y por la legislación interna[13].

Estos asuntos requieren que el nuevo marco normativo establecido por el RGPD abarque las peculiaridades que presenta cada uno de ellos. Ya no va depender directa o indirectamente de la voluntad del interesado que pueda darse nacimiento a datos de carácter personal. Por otro lado, la ley no puede prever con tanta facilidad la naturaleza que tendrán estos datos y en función

---

[11] V. sobre la discriminación en el ámbito de la salud, Castro Jover, Adoración, *Discriminación y salud*, en Romeo Casabona, Carlos María (Dir.), *Enciclopedia de Bioderecho y Bioética*, Ed. Comares - Cátedra Interuniversitaria de Derecho y Genoma Humano, Granada, España, 2011, T. I., pp. 672 y ss.

[12] V. art. 11 CDHB (Convenio de Oviedo) y el art. 4 de su Protocolo Adicional, relativo a *Genetic Testing for Health Purposes*, de 2008; art. 11 de la Declaración Universal sobre Bioética y Derechos Humanos, aprobada por la Conferencia General de la UNESCO el 19 de octubre de 2005.

[13] V. art. 14 de la Constitución y arts. 2, a) y 58.6 de la LIB.

de ella establecer su régimen jurídico específico. Las tareas relacionadas con la transmisión de información al titular de los datos pueden ser demasiado cortas o demasiado extensas.

En resumen, desde el punto de vista jurídico el *big data* presenta una relevante novedad y un gran desafío. Así, en primer lugar, debemos plantearnos si el marco jurídico actual, aun siendo nuevo, aporta una herramienta adecuada para regular situaciones nuevas y futuras que percibimos ya como previsibles a no muy largo plazo. En concreto, debemos dirigirnos al nuevo régimen establecido por el RGPD para obtener respuestas y más en particular para comprobar si son suficientes las que establece sobre el *big data*.

Estos mismos interrogantes se suscitan en el Derecho interno, para determinar si es necesaria una adaptación de las leyes actuales. En este sentido, la nueva normativa de nuestro país que complementa y desarrolla el RGPD, establece criterios y prescripciones adaptadas a las exigencias jurídicas específicas que se derivan de la aparición del *big data* en la sociedad. Queda pendiente comprobar si la actualización ha sido suficiente y acertada.

3. El dato relativo a la salud. Insuficiencias conceptuales

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, tanto en el marco normativo español[14] como en el europeo[15]. Dentro de los datos personales aquéllos relativos a la salud, los genéticos y los biométricos gozan de una especial y más intensa protección en el RGPD, si bien también se contemplan numerosas excepciones que relativizan este estatuto aparentemente privilegiado. De aquí se deriva la necesidad de precisar estos conceptos y esta forma de protección especial.

Como puede deducirse de la definición legal que proporciona el RGPD[16], el concepto de datos relativos a la salud discurre en un marco aparentemente limitado, pues incluye únicamente los datos relativos a la salud física o mental de una persona física que revelen información sobre su estado de salud. Sin

[14] Art. 18.4 CE, según interpretación del TC: SSTC 290/2000 y 292/2000, ambas de 30 de noviembre.

[15] V. arts. 8.1, de la Carta de los Derechos Fundamentales de la Unión Europea y 16.1 TFUE.

[16] Art. 4.15 RGPD: "Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

embargo, podemos encontrarnos con situaciones diversas que también se mueven en el ámbito de la salud, pero que no están explícitamente abarcadas por la definición legal, pero tal vez sí por vía interpretativa, siempre que no llegue a rebasar el marco legal[17].

Estado de salud presente y futura. En primer lugar, habrá que entender que se refiere no sólo al estado de salud presente, sino también futuro de la persona afectada, como puede ocurrir con la información predictiva que sobre la misma pueden aportar los análisis genéticos y la detección de ciertos biomarcadores presentes en el cuerpo de la persona implicada. No obstante, esta ampliación del concepto de salud no parece ser incompatible con la definición legal de dato de salud que proporciona el Reglamento.

Datos de carácter médico. El Grupo de Trabajo del Artículo 29[18] incluye bajo este concepto numerosos registros, como la historia clínica, resultados de pruebas diagnósticas, de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, información sobre discapacidades, padecimiento de una enfermedad o riesgo de padecerla, registro o adscripción al sistema público o concertado de salud o equivalente, etc.

Datos que circunstancial o indirectamente aportan información sobre la salud de una persona. Otra cuestión que se suscita para determinar con mayor precisión qué debemos entender por datos de salud es si pueden considerarse comprendidos dentro de los "datos relativos a la salud física o mental de una persona" aquéllos que circunstancial o indirectamente pueden aportar "información sobre el estado de salud de una persona", o que aporten información sobre su *previsible* (o futuro) estado de salud, sin que en sentido estricto tengan la naturaleza de tales. Así ocurre, por ejemplo, con los datos relativos al lugar de residencia (o zona o barrio, si ésta es urbana, p. ej., por razón de la existencia o no de infraestructuras sanitarias o de salubridad adecuadas) y al entorno medioambiental, al estilo de vida (actividades de ocio y de consumo, práctica de deportes, tipo de alimentación), a la actividad laboral o profesional del interesado, a sus relaciones económicas, entre otros.

---

[17] Téngase en cuenta el cndo. 35 del RGPD, que facilita la ampliación del concepto de datos de salud, aunque alguna de las variantes de las que se proponen a continuación en el texto no cuentan con un apoyo interpretativo suficientemente explícito en el mencionado cndo.

[18] Article 29 Data Protection Working Party, *Opinion 2/2013 on apps and smart devices*, 27 February 2013. V. también el cndo 35 del RGPD.

Es cierto que en sentido estricto podemos aceptar que aquéllos no son datos relativos a la salud física o mental de una persona, pero es evidente también la importancia que revisten para conocer con mayor precisión el estado de salud presente o futura de aquélla[19]. La limitación que presenta la definición mencionada no justifica en cualquier caso la exclusión de la misma de estos otros datos, pues ciertamente de ellos al menos puede deducirse información relevante para conocer o prever el estado de salud actual o futuro de una persona, por lo que la conclusión tendría que ser favorable a extender a esta categoría de datos de salud "circunstanciales o indirectos" el régimen de especial protección que otorga la norma a los datos de salud, pues, ciertamente, lo son *funcionalmente*.

En consecuencia, mi propuesta es afirmativa, es decir, su asimilación jurídica a los datos de salud en la medida y en cuanto estos datos o una parte de ellos se encuentren vinculados de forma permanente o temporal con aquellos y sean utilizados con propósitos o en contextos relacionados directamente con la salud[20]. Por consiguiente, en estos contextos, pero solo en ellos, los datos "circunstanciales o indirectos" relativos a la salud podrían asimilarse a los datos relativos a la salud, no en otros ajenos a la misma. Así, p. ej., si los datos relativos al lugar de residencia pueden aportar información relevante sobre la salud –presente o futura– de una persona determinada esa parte relativa al lugar de residencia podrá considerarse como dato relativo a la salud cuando se esté utilizando, por ejemplo, para hacer un diagnóstico o pronóstico sobre su salud, pero no para otros usos o en otros contextos.

¿Los datos del nasciturus *se corresponden con los de una persona física?* Desde el punto de vista subjetivo el titular de los datos (el interesado, art. 4.1 RGPD) ha de ser una persona física, prescribe el RGPD. No cabe discusión alguna sobre que haya de tratarse de una persona "física", es decir de un ser humano. Pero este ser humano ha de tener reconocida la condición jurídica de "persona", de acuerdo con lo que prevé el ordenamiento jurídico interno (Código Civil)[21]. Por consiguiente, *la titularidad de los datos relativos a la*

---

[19] Romeo Casabona, Carlos María (Coord.) / Nicolás Jiménez, Pilar / De Miguel Beriain, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en Medicina Personalizada de Precisión*, Fundación Instituto Roche, Madrid, España, 2018, p. 29.

[20] Próximo a la posición del texto Pérez Gómez, J.M., "Especialidades en el sector sanitario", *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, López Calvo, J. (Coord.), Wolters Kluwer, Madrid, España, 2018, p. 197.

[21] Art. 29 CC: "El nacimiento determina la personalidad, pero el concebido se le tiene por nacido para todos los efectos que le sean favorables, siempre que nazca con las condiciones que expresa el artículo siguiente". Art. 30: "La personalidad se adquiere en el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno".

salud también alcanza al concebido ("se le tiene por nacido para todos los efectos que le sean favorables"), indudablemente siempre condicionado a que se produzca el nacimiento.

Nuestra legislación específica contempla, en todo caso, los deberes de secreto en relación con los análisis que se hayan podido realizar sobre el embrión implantado y sobre el feto[22]. Este criterio lo venimos defendiendo especialmente en relación con los datos genéticos, dado su en principio carácter permanente e inmutable (van a perdurar inalterados a lo largo de toda la vida del ser humano, ya desde el momento de la concepción, a salvo de posibles mutaciones del ADN espontáneas, accidentales o provocadas, o de alteraciones epigenéticas), pues para garantizar la efectividad de la protección que les reconoce la ley ha de extenderse su manto protector desde el momento en el que se obtiene por primera vez esta clase de información en cualquier momento de la fase prenatal.

De acuerdo con el derecho interno, un régimen semejante habrá que aplicar al embrión in vitro mientras no se haya descartado del todo la posibilidad de incluirlo en un plan de reproducción asistida[23].

Conforme al nuevo régimen normativo europeo los derechos de los interesados, en particular los relacionados con los datos de salud, descansan en varios de carácter esencial, como son el consentimiento de los interesados, los principios de transparencia y comunicación (derecho a la explicación)[24] y el efectivo ejercicio de los llamados derechos ARCO (derechos de acceso, rectificación, cancelación y oposición).

4. La secuenciación masiva de genomas humanos: revisión del estatuto jurídico de los datos genéticos

Merece ser destacado en primer lugar que se incluyen en el RGPD los datos genéticos de forma explícita e independiente de los datos relativos a la salud, aportando incluso una definición de los mismos:

---

22 V. LIB, art. 53.

23 V. LIB, art. 53.

24 RGPD, art. 13.2, f): "Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: […] f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, *información significativa sobre la lógica aplicada*, así como la *importancia y las consecuencias previstas* de dicho tratamiento para el interesado".

> "Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona"[25].

Como es sabido, los datos genéticos presentan unas características muy particulares que los hacen diferentes de los demás datos vinculados con la salud y que justifican su tratamiento jurídico específico[26]: se encuentran en todas las células del cuerpo, salvo en los hematíes; son predictivos, inalterables (sin perjuicio de mutaciones espontáneas o provocadas) y únicos (con salvedad de los gemelos monocigóticos); las características genéticas que revelan se comparten en diversa medida con la familia biológica y se transmiten en diverso grado a la propia descendencia.

En consecuencia, de conformidad con el Reglamento, es indiscutible que se trata de datos personales, que es toda información sobre una persona física identificada o identificable[27]. Al mismo tiempo, son datos relativos a la salud[28], es decir, datos personales relativos a la salud física o mental de un ser humano, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud[29]. Aportan información sobre el origen racial o étnico y sobre el sexo (y en ocasiones tal vez también sobre la sexualidad) de las personas. Y, finalmente, son datos "sensibles"[30], entendiendo por tales aquéllos respecto a los cuales los interesados son más

---

[25] RGPD, art. 4.13. V. art. 4.14 para la definición de datos biométricos. El cndo. 34 del RGPD completa la definición: "[provenientes del análisis de una muestra biológica de la persona física en cuestión], en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente".

[26] En este sentido también el Grupo de Trabajo del Artículo 29 sobre Protección de Datos, *Documento de trabajo sobre datos genéticos*, adoptado el 17 de marzo de 2004.

[27] RGPD, art. 4.1.

[28] Pérez Gómez, J.M., "Especialidades en el sector sanitario", *op. cit.,* p. 199, encuentra la explicación a la distinción entre datos de salud y datos genéticos a su interés para la investigación científica, más que para la actividad asistencial, limitada en la actualidad al diagnóstico, lo que se corrobora porque es más relevante la regulación que se hace a ésta última en la Ley 14/2007 (LIB). Sin embargo, y al contrario, más abajo podremos comprobar que la finalidad de la investigación científica comporta, de acuerdo con el RGPD, un relajamiento de la protección de los datos personales, incluidos los genéticos, por dar prioridad al interés social frente al individual. La LIB dedica más atención a la investigación –genética–, porque forma parte de las competencias del Estado, frente a las más amplias que tienen atribuidas las CCAA en relación con la asistencia sanitaria.

[29] RGPD, art. 4.15 y 13.

[30] Como datos especialmente sensibles los califica el Grupo del Artículo 29 sobre protección de datos, *Documento de trabajo sobre datos genéticos*, *op. cit.*

vulnerables cuando se enfrentan a agresiones contra esta categoría de datos o contra otros derechos a través de los mismos.

Por esta razón el RGPD incluye estos datos en el grupo de "categorías especiales de datos". La consecuencia jurídica más importante es que queda prohibido el tratamiento de los datos personales que están recogidos en esta categoría especial de datos: los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de *datos genéticos*, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. Salvo que se cuente previamente con el consentimiento del interesado.

Este tratamiento jurídico reforzado de los datos genéticos cuenta, no obstante, con algunas excepciones, como cuando el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social[31]; o cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios[32]. De todos modos, se establece el deber de confidencialidad en ambos casos[33].

Existe un conjunto de garantías y derechos que protegen la autonomía y privacidad del paciente y su familia, previenen la discriminación a causa de las características genéticas, garantizan la equidad en el acceso a la atención sanitaria y el derecho a la explicación (información sobre la lógica del procesamiento de los datos mediante sistemas inteligentes automáticos)[34] y a la información y al consentimiento[35], etc.

Sin perjuicio de lo indicado, es necesario mantener un equilibrio entre estos derechos y las necesidades clínicas asistenciales y de investigación, como son el acceso al material biológico humano (muestras biológicas), a

31 RGPD, art. 9.2, h.
32 RGPD, art. 2, i.
33 RGPD, art. 9.3.
34 RGPD, art. 13.2, f), transcrito más arriba.
35 RGPD, arts. 7 y 8.

los datos obtenidos, transferencia y comunicación de los mismos con otros profesionales, etc.[36].

Puede ser una necesidad para la investigación biomédica fomentar el libre flujo de datos a través de silos y reducir las complejidades en torno al consentimiento del paciente. A veces pueden surgir tensiones para conciliar ambos intereses.

La primera garantía establecida por la ley consiste en imponer límites a la realización de pruebas genéticas. Pero estos límites los encontramos ya con anterioridad a la aprobación del RGPD en el CDHB (art. 12) y en la LIB (art. 9).

El tratamiento de datos genéticos presenta diversos problemas jurídicos específicos:

1. La protección de los datos obtenidos por medio de la secuenciación de genes o de segmentos o secuencias de los mismos (privacidad).

2. La vinculación de datos aparentemente no relacionados (datos anónimos e identificados o identificables; datos anónimos entre sí) (privacidad).

3. La transmisión al paciente de la información obtenida (deber de información sobre los hallazgos obtenidos).

4. Autonomía y consentimiento del interesado.

[36] RGPD, art. 89, establece las garantías y límites sobre el acceso y uso de los datos con fines de investigación científica. En cuanto a las garantías alude a la seudonimización, en la medida en que pueda garantizar los fines que se mencionan. Como se podrá comprobar más abajo, no parece ser éste un instrumento suficientemente eficaz para proteger los derechos de los interesados. Por otro lado, ha sido erróneo el reconocimiento a los EM de iniciativas legislativas sobre este particular, pues podrá favorecer diferencias y desigualdades normativas entre aquéllos, aunque se mantiene explícitamente la competencia regulativa de la UE, lo que podría paliar o corregir estas desviaciones. Un estudio extenso y en detalle sobre las diversas aristas que presenta este complejo precepto, v. Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, cit. Abundante información complementaria en Bensoussan, A. (Dir.), *Règlement Européen sur la protection des données. Textes, commentarires et orientations pratiques*, Larcier, Bruxelles, 2016, pp. 430 y ss.

5. Deberes de los profesionales de la salud, principalmente vinculados con la confidencialidad y con la revisión y validación previas de las propuestas del sistema automatizado.

6. Otras preocupaciones (relevancia de las pruebas genéticas masivas en relación con la medicina reproductiva; acceso a nuevas técnicas avanzadas por parte de los pacientes).

7. La posibilidad cesión remunerada de datos a compañías del sector o prestadoras de servicios específicos de almacenaje y tratamiento de datos de salud a cuenta de terceros (centros sanitarios)[37].

Los datos genéticos, por tanto, también los procedentes de la secuenciación genética masiva, pertenecen a una categoría especial de datos, reconocida por el RGPD.

Aclarado lo anterior, hay que identificar a continuación cuáles son los derechos e intereses del titular de los datos y/o del llamado sujeto fuente de la muestra biológica que pueden verse comprometidos. Este segundo aspecto configura lo más novedoso, tanto desde el punto de vista de la investigación científica como de su tratamiento jurídico.

Si puede aceptarse sin discusión que son legalmente datos genéticos tanto las características genéticas heredadas como adquiridas (p. ej., por efectos epigenéticos o por mutaciones exógenas, como radiaciones de origen diverso), no está tan claro que acoja aquella parte del ADN que no contiene genes (o secuencias de los mismos), es decir, el ADN no codificante. En efecto, si este ADN no aporta información sobre las características genéticas de una persona referentes a su fisiología o a su salud, debería descartarse su asimilación en la definición legal de dato genético. En efecto, este ADN, al menos hasta lo que se conoce de él en la actualidad, no aporta este tipo de información, a salvo de la identificación de la etnia y del sexo; no obstante, este último puede ser relevante para el conocimiento de las enfermedades vinculadas con el sexo.

---

[37] V. sobre esta cuestión, Romeo Casabona, Carlos María / Nicolás Jiménez, Pilar / De Miguel Beriain, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en Medicina Personalizada de Precisión*, *op. cit.,* pp. 44 y ss.; Llàcer, M.R. / Casado, M. / Buisan, L., (Coords.), *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Observatori de Bioètica, Universitat de Barcelona, Barcelona, España, 2015, pp. 36 y ss.

De todos modos, el ADN no codificante contiene información de carácter personal que debe ser reconocida como objeto de protección por el Reglamento. No se olvide que a partir de este ADN se obtienen los perfiles del sujeto del que provienen para su identificación como posible implicado en un hecho delictivo (véase, no obstante, la aclaración a este respecto de más abajo) o para determinar la paternidad. Por consiguiente, es probable que no se les pueda aplicar el estatuto jurídico especial reconocido a los datos genéticos[38], pero si gozarán en todo caso de la protección establecida para los datos personales en general[39] (no la muestra biológica hallada en el escenario del crimen o en el cuerpo de la víctima, mientras no se identifique a la persona a la que pertenece), pero en estos casos es aplicable el régimen especial que establece la normativa sectorial[40].

Hechas estas consideraciones, debe tenerse en cuenta que el Reglamento excluye de su ámbito de aplicación material el tratamiento de los datos realizados en el curso de una investigación penal, lo que afectará a los datos obtenidos con estos fines del ADN no codificante[41].

Obsérvese que el RGPD se refiere que los datos genéticos pueden ser obtenidos mediante análisis de las muestras biológicas pertenecientes al mismo sujeto. A este respecto, la muestra biológica, en cuanto que es el continente de información genética y sobre la salud de la persona de la que proviene, debe gozar del mismo estatuto especial que estos datos.

---

[38] Al permitir el ADN no codificante identificar el sexo y la etnia del sujeto interesado, que pueden ser relevantes para el mejor conocimiento de enfermedades ligadas a alguno de estos parámetros, en estos casos gozarían de la naturaleza de datos relativos a la salud.

[39] V. sin embargo, Pérez Gómez, J.M., "Especialidades en el sector sanitario", *op. cit.,* pp. 198 y s., quien asimila toda la información proveniente del ADN al dato genético.

[40] V. Romeo Casabona, Carlos María / Romeo Malanda, Sergio, *Los Identificadores del ADN en el Sistema de Justicia Penal,* Thomson Reuters - Aranzadi, Pamplona, España, 2010, pp. 20 y ss.; AAVV., *Making sense in Forensic Genetics*, Euroforgen, Londres, Reino Unido, 2017. pp. 16 y ss.; García, O. *et ál.,* "Identificación de sospechosos a través de búsquedas familiares en la base de datos de ADN de interés criminal. Implicaciones sociales, éticas y científicas", *Rev Esp Med Legal*, Vol. 43, 2017, pp. 26-34.

[41] RGPD, art. 2.2, d: "El presente Reglamento no se aplica al tratamiento […] de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención." V. art. 326 y concordantes de la Ley de Enjuiciamiento Criminal, y LO 10/2007, de 8 de octubre.

5. Revisión del estatuto jurídico sobre el tratamiento de los datos de salud. Respuestas a los nuevos riesgos

5.1. Clasificación de las personas en grupos o subgrupos de acuerdo con sus perfiles personales

La posibilidad creciente de utilizar datos masivos de las personas y de incorporar también masivamente los datos de éstas a sistemas informáticos y a bases de datos permite agruparlas conforme a unas características predeterminadas, pudiendo obtener de este modo un perfil de estas personas que se comparten con otras, realizar estudios sobre las mismas, depurar algunos aspectos o manifestaciones de su personalidad y realizar predicciones sobre su comportamiento previsible, al menos en determinados ámbitos delimitados.

El RGPD describe con claridad qué debe entenderse por la elaboración u obtención de perfiles de las personas:

> "Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física"[42].

No cabe duda que clasificaciones de la población de acuerdo con ciertos patrones o perfiles previamente establecidos puede ayudar de manera muy eficiente a planificar y tomar decisiones en el sector privado, como orientar sus estrategias en el mercado para implementar la producción de ciertos productos y, en este caso también en el sector público, las prestaciones de determinados servicios o, por el contrario, para reducir o abandonar otros. Como sabemos, estas estrategias y sus objetivos no son nuevos, pero las TIC favorecen su desarrollo y la mejora de su precisión y eficacia.

Su utilidad específica en el sector de la salud es indudable. Así, puede ayudar a la obtención de ciertos perfiles en el ámbito sanitario asistencial para la elaboración de protocolos, siempre científicamente respaldados, que señalen pautas de actuación de los profesionales de la salud (p., ej., sobre la prescripción por el facultativo de pruebas diagnósticas ante un

[42] RGPD art. 4.4.

cuadro estándar –de perfil– que presente un paciente; o sobre el tratamiento adecuado para ese perfil, más que para el paciente concreto).

Nada hay que objetar en principio a estas acciones y a esta forma de utilización de los recursos tecnológicos en el tratamiento de los datos, en particular si son anónimos o han sido anonimizados, en concreto en este último caso cuando están destinados a la investigación científica. Más dudoso es que estas estrategias y la disponibilidad de TIC avanzadas promuevan la toma de decisiones rutinarias o, peor, completamente automatizadas, sin otro tipo de respaldos que refuercen la decisión o la desaconsejen; o se focalicen hacia personas concretas que responden al perfil que interesa identificar.

En concreto son rechazables por lo que estas estrategias pueden comportar de intrusión en la esfera privada de las personas o en la autonomía decisional de los pacientes, al limitar o excluir que éstos puedan tomar una posición sobre la propuesta decisional del sistema inteligente, incluso oponiéndose a ella. Aquí podría llegar a imponerse el imperativo tecnológico sobre la libertad del paciente de aceptar o de rechazar un tratamiento, y vulnerar de este modo los derechos que le reconocen las leyes[43].

En principio una regulación normativa que asegure una limpieza en el uso de las TIC en estos contextos clasificatorios parece estar reservado a un marco normativo que va más allá del relativo a la protección de datos de carácter personal, pero cuyo estudio desde esta perspectiva más amplia tendrá que abordarse.

Un problema jurídico de primera magnitud, que podrá afectar también a los pacientes, se refiere a que la elaboración de perfiles a partir de datos personales tienda a clasificar de forma consecuente a las personas en grupos o subgrupos con perfiles similares a los que se asocian determinados patrones; p. ej., incluir a un paciente oncológico en protocolos que se refieren a las actuaciones asistenciales para cuadros cancerosos semejantes sin tener suficientemente en cuenta las variantes que pueda presentar ese paciente concreto.

A partir de ahí podrían asumirse decisiones automatizadas por parte de los profesionales asistenciales, prescindiendo de individualizar la decisión, esto es, de las características más singulares o individuales que presente

[43] V. Ley 41/2002, art. 8, relativo al consentimiento informado. El RGPD enfatiza la importancia que se otorga al consentimiento, que pasa por su propia definición (art. 4.11); v. también el cndo. 35 y art. 9.2, a), entre otros.

el paciente en cuestión, sin supervisar y validar, en su caso, las propuestas decisionales del sistema digital. Sobre este particular la conclusión no puede ser otra que rechazar que una decisión asistencial esté basada exclusivamente en perfiles elaborados sobre los pacientes y se tome de forma exclusivamente automatizada, sobre todo si conduce a la exclusión del tratamiento sin ofrecer a cambio otro supuestamente menos eficaz pero indicado como alternativa[44]. En consecuencia, podrían ser víctimas de prácticas arbitrarias, al no tener en cuenta otros elementos decisorios relevantes; o discriminatorias, al poder ser excluido de un tratamiento o prescribirle otro en atención a diversas consideraciones extra sanitarias. Sin embargo, no significa esta reflexión que toda práctica automatizada deba ser acreditada o revalidada, pues comportaría un retroceso; solo cuando la decisión pueda implicar una afectación de la integridad o salud del paciente, como se indicará a continuación.

5.2. Tendencia a tomar decisiones automatizadas de las personas

El tratamiento automatizado de datos personales, en particular su procesamiento mediante algoritmos y la tecnología del *big data*, puede incrementar la tendencia a aceptar automáticamente propuestas de decisiones concretas; quiere decirse, asumir decisiones elaboradas por el sistema inteligente sin supervisarlas o contrastarlas a la luz de la situación concreta del paciente y su entorno. Significa ello admitir, al menos como hipótesis, que se proceda a tomar las decisiones que el sistema artificial proponga, sin una revisión o supervisión *humana* previas con la cualificación que corresponda, y sin fundamentar o explicar por qué se ha llegado a esa conclusión; dicho de otro modo, sin valorar la perspectiva causal (o, si se prefiere, la fundamentación) que comporta todo proceso decisional[45]. Como señalaba más arriba, la elaboración de perfiles clasificatorios de las personas con la ayuda de sistemas de inteligencia artificial propicia este tipo de comportamientos.

Es previsible que se vayan extendiendo decisiones automatizadas en el sentido vedado por el Reglamento[46], empezando por los procesos decisio-

---

[44] Romeo Casabona, Carlos María / Nicolás Jiménez, Pilar / De Miguel Beriain, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en Medicina Personalizada de Precisión*, *op. cit.,* p. 37.

[45] En este sentido, Gil González, E., *Big data, privacidad y protección de datos*, AEPD y BOE, Madrid, España, 2016, p. 42.

[46] RGPD, art. 22.1: "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Mientras que el apartado 2º admite que pueda prestar su consentimiento el interesado a esta forma decisional o que medie un contrato entre aquél y el responsable del trata-

nales más sencillos y tal vez irrelevantes, pero que probablemente avanzarán a terrenos más complejos.

La tendencia a reconocer rutinariamente propuestas de decisiones concretas a partir del tratamiento automatizado de datos personales, en particular su procesamiento mediante algoritmos y la tecnología del *big data*, podrá incrementarse; quiere decirse, asumir decisiones elaboradas por el sistema inteligente sin supervisarlas o contrastarlas a la luz de la situación concreta del paciente y su entorno. Significa ello admitir, al menos como hipótesis, que se proceda a tomar las decisiones que el sistema proponga, sin una revisión o supervisión *humana* previas con la cualificación que corresponda, y sin tratar de fundamentar o explicar por qué se ha llegado a esa conclusión; dicho de otro modo, sin valorar la perspectiva causal (o, si se prefiere, la fundamentación) que comporta todo proceso decisional[47]. Como señalábamos más arriba, la elaboración de perfiles clasificatorios de las personas con la ayuda de sistemas de inteligencia artificial propicia este tipo de comportamientos.

Algunas empresas privadas están trabajando en el perfeccionamiento de sistemas computacionales capaces de establecer relaciones de datos diversas que al mismo tiempo permitan a la persona responsable de la toma de la decisión seguir el proceso al que ha llegado a favor de una determinada decisión y no a favor de otra, como puede ocurrir al dictaminar un diagnóstico médico (así, con la Plataforma Watson, de IBM; o con la de Google). Esta información daría confianza al profesional en el momento de aceptar el diagnóstico establecido por el sistema y tomar a partir de él las decisiones asistenciales oportunas[48]. Sin embargo, no parece tarea fácil salirse de la rutina y que el profesional revise con la atención suficiente el proceso decisional seguido por el sistema en el manejo de los algoritmos. Conseguir

---

miento, el apartado 3º excluye la automatización, aunque medie el consentimiento o el contrato indicados cuando se trata de datos especiales (art. 9.1), entre los que figuran los datos de salud y los genéticos. Este último apartado establece que el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. V. sobre este particular Maier, N. / Ossoining, V., "Einzelne Bereiche der Datenverarbeitung", *Europäische Datenschutz-Grundverordung*, Rossnagel, A. (Hrsg.), Nomos Verlag, Baden-Baden, Alemania, 2017, p. 226, aunque no tienen en cuenta la excepción prevista en el apdo. 3 al consentimiento del interesado, como se acaba de indicar.

[47] En este sentido, Gil González, E., *Big data, privacidad y protección de datos*, AEPD y BOE, Madrid, España, 2016, p. 42.

[48] Gil González, E., *Big data, privacidad y protección de datos*, *op. cit.,* p. 42 y s.;

que la tecnología sea capaz de aportar más información sobre este proceso será el reto principal para prevenir automatismos decisionales.

En conclusión, cualquier decisión o propuesta decisional apoyadas en la información proporcionada por un sistema basado en el procesamiento automatizado de algoritmos, que comporte algún riesgo apreciable para la salud del paciente, deberán ser adoptadas y/o *supervisadas por un ser humano cualificado*, de modo que pueda valorar su decisión a la luz de la situación concreta que presente el interesado (p. ej., no limitarse a excluir a un paciente de un tratamiento novedoso porque de acuerdo con su perfil no va a resultarle beneficioso, sino reconsiderar la decisión propuesta y asegurarse de la conveniencia de optar por otro tratamiento alternativo con la potencialidad de aportar algún beneficio para tratar la enfermedad).

De acuerdo con la normativa europea, una decisión asistencial, por ejemplo, no podrá basarse exclusivamente en los perfiles obtenidos del paciente; esta prohibición es coherente con la esencia de individualización de la que parte una nueva concepción de la medicina que se está abriendo camino: la Medicina Personalizada de Precisión[49]. Se considera que esta perspectiva metodológica, de base personal e individualizada, constituye el medio más adecuado, si se actúa de forma coherente con lo que ella representa, para prevenir la asunción de conclusiones equivocadas en la que también puede incurrir un sistema computacional, conclusiones que a su vez podrían conducir a la toma de decisiones también equivocadas[50].

En esta dirección apunta con claridad la nueva normativa europea, al imponer que todo interesado tendrá derecho a no ser objeto de una decisión basada *únicamente* en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar[51]. No cabe duda de que un paciente puede verse seriamente

---

[49] Romeo Casabona, Carlos María (Coord.) / Nicolás Jiménez, Pilar / De Miguel Beriain, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en Medicina Personalizada de Precisión*, *passim.*

[50] Romeo Casabona, Carlos María (Coord.) / Nicolás Jiménez, Pilar / De Miguel Beriain, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en Medicina Personalizada de Precisión*, *op. cit.,* pp. 61 y ss.

[51] RGPD, art. 22.1: "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Mientras que el párrafo 2º admite que pueda prestar su consentimiento el interesado a esta forma decisional o que medie un contrato entre aquél y el responsable del tratamiento, el párrafo 3º excluye la automatización, aunque medie el consentimiento o el contrato indicados cuando se trata de datos especiales (art. 9.1), entre los que figuran

comprometido por cualquier decisión que repercuta en sus expectativas y que puede afectarle "significativamente" en cada una de las situaciones en las que pueda encontrarse.

5.3. La seudonimización como vía de protección de datos personales

El RGPD otorga una significativa relevancia jurídica a la figura de la seudonimización, como alternativa a otros procedimientos más explícitos y directos para la protección de datos personales[52], pues se trata de disponer de un mecanismo que garantice en cierta medida dicha protección y al mismo tiempo no obstaculice la investigación científica[53]. Es otra de las novedades que incorpora el propio Reglamento[54], empezando por aportar una definición de seudonimización:

> "El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"[55].

Esta definición de seudonimización, aunque no utiliza expresamente la expresión "disociación", como el procedimiento habitual de separación de los datos de identificación de los demás que pertenecen a una misma persona, lleva implícita tal proceso. En efecto, la posibilidad de reidentificación que deja abierta la definición de seudonimización requiere una información adicional que facilite volver a vincular los datos propiamente identificativos con los demás datos.

---

los datos de salud y los genéticos. Este último apartado establece que el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. V. sobre este particular Maier, N. / Ossoining, V., "Einzelne Bereiche der Datenverarbeitung", *Europäische Datenschutz-Grundverordung*, Rossnagel, A. (Hrsg.), Nomos Verlag, Baden-Baden, Alemania, 2017, p. 226, aunque no tienen en cuenta la excepción prevista en el apdo. 3 al consentimiento del interesado, como se acaba de indicar.

52 V. más ampliamente, Romeo Casabona, Carlos María, "Anonymization and Pseudonymization: The Legal Framework at a European Level", *The Data Protection Directive and Medical Research Across Europe,* Beyleveld, D. / Townend, D. / Rouillé-Mirza, S. / Wright, J. (Eds.), Sheffield Institute of Biotechnological Law and Ethics, Ashgate, 2004, pp. 33-50.

53 V. Pérez Gómez, "Especialidades en el sector sanitario", *op. cit.,* p. 204.

54 Esta novedad normativa es reconocida por el propio RGPD en su cndo. 28.

55 RGPD art. 4.5.

El peso de la definición recae en dos aspectos: en el hecho de la existencia de esta información *adicional*; y en que se encuentre *separada* y sometida a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyan a una persona identificada o identificable; o, dicho de otro modo, que tales medidas no permitan la identificación de la persona a la que se atribuyan por ese procedimiento de asociación, sin utilizar una información adicional. En todo caso, por una persona distinta a quien ejerce el control legal sobre el uso de esa información adicional[56].

La información adicional a la que se refiere el RGPD puede ser cualquiera que permita vincular –o desvincular, si se prefiere– unos y otros datos, es decir, los identificativos con los demás: un código, una clave o contraseña, etc.

El concepto jurídico de seudonimización se proyecta de forma directa sobre los datos, pero se halla muy ligado también a otros conceptos con los que guarda una gran proximidad, como sucede, según se ha indicado, con el de disociación de los datos e, indudablemente, con el de anonimización, aunque éste no lo mencione el RGPD. También ocurre con las expresiones de persona identificada o identificable, que aluden a los sujetos titulares de los datos[57]. Por tal motivo, deberemos continuar profundizando sobre estos conceptos, así como sobre el alcance jurídico real de la protección de los datos en el contexto y entorno de procesos de seudonimización de los mismos, pues continúan siendo datos personales objeto de protección por el Reglamento[58].

Por lo demás, la seudonimización es uno de los recursos que prevé el RGPD para hacer factible las excepciones a las garantías previstas sobre los datos personales relativos a la salud y a los datos genéticos cuando se prevé el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[59], de modo que se logren los objetivos propuestos[60].

---

56 Es el responsable de los datos quien debe indicar las personas que están autorizadas para tratar estos datos y tener acceso a la información adicional: RGPD cndo. 26.

57 V. RGPD, art. 4.1.

58 En este sentido, Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, cit.

59 RGPD, art. 89.1 y 2.

60 RGPD, cndos. 28 y 29.

En esta materia, además, el Reglamento reconoce una amplia capacidad normativa a los Estados Miembros y a la propia UE[61]; lo que no deja de ofrecer dudas sobre el acierto de esta medida, al menos en el sector de la investigación biomédica, pues ya conocemos que una disparidad normativa entre los EM puede ser perturbadora, aunque se muevan dentro de un marco legal común (el RGPD). En efecto, se puede dificultar la cooperación entre ciudadanos (grupos de investigadores) de países con especificaciones legales discrepantes, como es precisamente la cesión de datos con fines de investigación científica biomédica entre investigadores, cada vez más habitual. No obstante, el RGPD prevé que "el Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos"[62].

5.3.1. El régimen normativo de la seudonimización

La seudonimización se diferencia de la anonimización en que, consistiendo en el tratamiento de datos, comporta un procedimiento reversible de disociación de aquéllos, y la persona a la que pertenecen éstos es identificable en el sentido que le otorga la normativa europea. Sin embargo, los efectos jurídicos de la seudonimización han cambiado con el actual marco legal.

En los supuestos de cesión de datos, el RGPD consagra el principio de cesión de los datos seudonimizados, en varios supuestos, entre ellos la investigación científica. El RGPD no requiere en la actualidad un consentimiento añadido cuando el investigador procede a una cesión a terceros (p. ej., a otros investigadores que trabajan en el mismo proyecto, sea en el mismo centro o en otros), que era una de las trabas principales con las que se enfrentaban los científicos cuando trabajaban en colaboración con otros grupos o equipos de diferentes centros, incluso del espacio europeo.

---

61 RGPD, art. 89.2. Así lo corrobora Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, *op. cit.*

62 RGPD, cndo. 53.

Sin perjuicio de lo ya indicado, el nuevo régimen establecido en 2018 por la LOPDGDD para el uso de datos con fines de investigación biomédica tiene como uno de sus pilares básicos la seudonimización, tratamiento que ya se preveía desde 2007 en la LIB. Al menos en el ámbito de la salud, para el que se regula específicamente, puede sostenerse que no existe una completa concordancia con el RGPD, como se va a explicar a continuación.

Conforme a la LOPDGDD se considera lícito el *uso* –según expresión de la Ley citada– de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica[63]. Es decir, cuando los datos estén previamente seudonimizados no es preciso el consentimiento del interesado, puesto que el tenor literal dice exactamente "el uso de datos personales seudonimizados", esto es, el uso de datos que *ya están* seudonimizados, es decir, con anterioridad; no basta (el proceso de) la seudonimización de datos personales para su subsiguiente uso, mejor diríamos tratamiento, que abarca más conductas y es más correcto en términos jurídicos. Sin embargo, el legislador interno está obligado a conocer la diferencia legal existente entre "uso" y "tratamiento", por lo que debemos dar su relevancia interpretativa a que se haya recurrido a un término y no al otro, no puede entenderse casual (aunque también pudiera responder a un mero defecto de redacción, que en esta ocasión entiendo descartable) [64].

La poco clara redacción de esta parte de la Ley suscita una duda importante que he resuelto en una determinada dirección. Aquélla consiste en despejar si para el proceso mismo de seudonimización es necesario el consentimiento del interesado; o si no requiere dicho consentimiento. En coherencia con la posición que he mantenido[65] de que la LOPDGDD exige de

---

63 Disposición Adicional 17.2, d), LO 3/2018.

64 El empleo de la terminología adecuada ha sido descuidado por el legislador interno, puesto que es obvio que el uso de datos según la ley va más allá del significado estricto de esta palabra, como son la cesión, transformación, etc., que el legislador comunitario sintetiza en la definición de "tratamiento" (como ya hiciera en la Directiva de 1995): "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art. 4.2 del RGPD). El jurista no puede dejar de sentir perplejidad ante tan importantes imprecisiones e incorrecciones, que lastran la comprensión del sentido del texto de la ley.

65 V. Romeo Casabona, Carlos María, "El Nuevo marco normativo europeo sobre protección de datos personales y el estatuto de las muestras biológicas humanas y de los biobancos para investigación biomédica", *Comunicaciones en Propiedad Industrial y Derecho de la*

forma general el consentimiento del interesado para el tratamiento de datos con fines de investigación en salud y en particular biomedicina, y de que la Ley sólo se refiere al uso y no al tratamiento de datos –ya– seudonimizados, la primera opción parece más adecuada respecto al tenor literal del texto legal, es decir, es necesario el consentimiento del interesado para proceder a la seudonimización; pues aunque la segunda es también plausible, y tal vez fuera lo que quiso expresar la Ley y probablemente también lo deseable, el texto legal no le confiere un apoyo evidentemente más fuerte que el primero[66].

Por consiguiente, la obligación general inicial de obtener el consentimiento del interesado no desaparece, aunque se haya previsto la seudonimización de aquéllos; tal obligación decae solo a partir del momento inmediatamente posterior a la culminación de su seudonimización. Ahora bien, podrá explicarse al interesado la finalidad del tratamiento de los datos respecto a una investigación concreta, pero bastará también con que su titular acepte la seudonimización, sea cual fuere el tipo de investigación (p. ej., biomédica) y el número de proyectos para la que vayan a utilizarse las muestras o los datos. La ventaja añadida que tiene la seudonimización es precisamente ésta, que podrán usarse los datos sometidos a este proceso, aunque no se haya informado al titular de los datos sobre el objetivo específico de las diversas investigaciones que puedan realizarse en el futuro. Y esta descarga incluye la cesión a terceros.

La cesión a terceros requerirá, además, el cumplimiento por parte del cesionario de ciertos compromisos que eviten la reidentificación, como se dirá más abajo.

El procedimiento de seudonimización es de gran utilidad y por ello defendible en algunos sectores, como la investigación biomédica, pues con su aplicación se facilita el acceso a los datos para esta última finalidad.

Los comités de ética de investigación biomédica podrían constituirse como intermediarios entre los investigadores, monitores y promotores, por

Competencia, Núm. 86, 2019, pp. 215-238; el mismo, "The new European legal framework on personal data protection and the legal status of biological samples and biobanks for biomedical research purposes in Spanish Law", *Article 89 of the General Data Protection Rule and biobanking in Europe*, Slokenberga, S. / Tzortzatou, O. / Reichel, J. (Eds.), Springer, Alemania (en prensa).

66 Romeo Casabona, Carlos María, "El Nuevo marco normativo europeo sobre protección de datos personales y el estatuto de las muestras biológicas humanas y de los biobancos para investigación biomédica", *op. cit.,* pp. 226 y ss.

un lado, y los pacientes, por otro, de modo que puedan defender y equilibrar los intereses de ambas partes, asumiendo que a su vez los miembros de estos comités están obligados legalmente por deberes de confidencialidad o de secreto[67].

La seudonimización debe cubrir los datos de identificación del interesado, así como los datos de identificación de localización (también los subdirectorios y objetos condicionados).

Los datos seudonimizados gozan, sin la menor duda, de la aplicación de los principios de la protección de datos personales. No en vano mantienen la característica de ser atribuibles a una persona identificable. Como puede apreciarse a lo largo de este estudio, un asunto diferente es que la protección jurídica en el caso de los datos seudonimizados pueda ser más relajada o limitada, en general o en algunas circunstancias especiales. Más arriba se vio cómo así lo establece sin ambigüedades el RGPD: los datos seudonimizados son datos de personas identificables y éstos gozan de protección normativa, pero limitada.

Cuándo pueden considerarse los datos atribuibles a una persona identificable se establece de este modo: "Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física"[68].

También da respuesta el RGPD a la cuestión de cómo se puede determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física: "deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos"[69].

---

[67] Sobre este particular ya me pronuncié en Romeo Casabona, Carlos María, "Utilización de muestras biológicas y bancos para la investigación biomédica", *Salud y Derecho. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados,* Brena Sesma, Ingrid (Coord.), Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, México, D.F., 2005. V. también, Instituto Roche: *Guía práctica para la utilización de muestras en investigación biomédica*, Madrid, España, 2006. La LIB y el RD 1716/2010 acogen este tipo de soluciones en varios de sus preceptos, algunos ya citados.

[68] RGPD cndo. 26.

[69] RGPD cndo. 26.

5.3.2. La anonimización y el estatuto jurídico de los datos anónimos y anonimizados

El RGPD no aporta un concepto de anonimización, aunque puede deducirse del concepto mismo de seudonimización[70]. No obstante, continúa presente de manera implícita (es decir, sin utilizar este término, pero sí su descripción) en los considerandos del Reglamento[71]. En todo caso, consiste en un proceso (procedimientos, por lo general técnicos, que concluyen en la eliminación irreversible de los elementos que permiten la identificación del sujeto implicado); no describe meramente una situación (la de dato anónimo o anonimizado).

La anonimización, en sentido estricto, implica también un tratamiento de datos, es decir, el procedimiento de disociación o separación de datos inicialmente atribuibles a personas identificadas o identificables, pero en este caso ha de desligar de forma definitiva e irreversible unos y otros datos, según nos referíamos en el apartado precedente.

El resultado de este tratamiento es que los datos tratados son –se vuelven– anónimos, pues no existen datos adicionales referentes al interesado que deban mantenerse separados. Por otra parte, también son datos anónimos los no identificables en origen, es decir, cuando fueron recogidos de este modo, o cuando con posterioridad se ha producido por cualquier motivo la destrucción del nexo de asociación entre los datos identificadores y los demás.

Como es sabido, las expresiones "identificable" ("no identificable", diríamos con mayor propiedad) y "anonimización" no incluyen el presupuesto de que sea absolutamente imposible la identificación del sujeto, sino que únicamente aluden a las medidas que permitan la identificación que sean "razonables"; por contra excluye las que para lograr la identificación del sujeto requieran "un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados"[72].

---

[70] Sí lo hace la LIB respecto a "anonimización" ("proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere"), "dato anónimo" y "dato anonimizado o irreversiblemente disociado". Cfr. el art. 3, letras c, i y h. Nótese que estas definiciones están redactadas con un planteamiento general, es decir, no circunscrito al ámbito de la investigación biomédica, sin perjuicio de la definición específica correspondiente de muestra biológica, que si se sitúa en este marco. En todo caso, se trata de una ley sectorial.

[71] V. RGPD cndo. 26.

[72] Así expresa literalmente esta idea la Ley 14/2007, en art. 3, i.

El criterio de la anonimización "razonablemente" irreversible es el que ha de prevalecer frente al mencionado en primer lugar, dado que es aceptado de forma unánime que es prácticamente imposible lograr una anonimización de los datos de forma absolutamente irreversible, salvo, quizá reduciendo drásticamente su contenido, lo que tendría como efecto no deseable la escasa utilidad que tendrían entonces esos datos para la investigación u otros fines reconocidos legalmente.

Por consiguiente, si unos datos personales han sido sometidos a tal proceso de anonimización de modo que ya no permiten razonablemente la identificación de la persona de la que provienen, a partir de ese momento dejarán de estar bajo la cobertura jurídica sobre protección de datos.

Así lo indica expresamente el RGPD: "Los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación"[73].

La anonimización no es un procedimiento completamente inocuo, pues podría desencadenar un doble efecto perjudicial para la persona afectada: una vulnerabilidad por deficiencia o ineficacia de las medidas de seguridad técnicas adoptadas; y una vulnerabilidad por falta de protección jurídica en ciertas situaciones en las que dicha anonimización podría ser reversible y daría lugar a la identificación del interesado, prescindiendo ahora de cuán complicado fuera tal procedimiento de reversibilidad.

Finalmente, si esos datos anónimos volvieran a ser vinculados con los que permiten identificar a la persona de la que provienen, utilizando para tal fin medios no razonables o esfuerzos desproporcionados o, incluso, aunque se produjera de forma accidental, esos datos recuperan de nuevo la categoría de datos personales, de acuerdo con la definición que establece el RGPD (art. 4.1), y les son aplicables otra vez los principios y reglas jurídicas de protección de los datos personales. A la misma conclusión deberá llegarse si mediante cualesquiera circunstancias o procedimientos ocurre que la persona

[73] RGPD cndo. 26.

es identificable (es decir, todavía no identificada, pero sí potencialmente) por procedimientos razonables[74].

5.3.3. El procedimiento de disociación

El concepto de seudonimización[75] y el procedimiento de disociación o separación de los datos de identificación de los demás datos eran ya conocidos en nuestra legislación anterior al RGPD. La LOPD definía como procedimiento de disociación todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (art. 3, f)[76]. En términos semejantes y más precisos se pronuncia la LIB para el sector de la Biomedicina[77].

La disociación de los datos presupone, por consiguiente, que han sido sometidos intencionadamente a tal proceso, lo que comporta el tratamiento de los mismos en el sentido de este precepto del RGPD, con el efecto de que "que ya no puedan atribuirse a un interesado sin utilizar información adicional", recordemos que dice el art. 4.5, con el propósito de proseguir su tratamiento finalista sin la carga que comporta disponer al mismo tiempo de los datos de identificación del interesado, en particular cuando estos últimos no son necesarios para la consecución del fin legítimo. De ella hay que distinguir cualquier otra situación que haya dado lugar de forma accidental o fortuita a la pérdida de la identidad del titular de los datos.

Los procedimientos de disociación pueden ser diversos (mediante pseudónimos, la codificación o cifrado de los datos de identificación, incluida la

---

[74] Ya en este sentido, Romeo Casabona, Carlos María, *Anonymization and Pseudonymization: The Legal Framework at a European Level, op. cit*., pp. 45 s.

[75] Recordemos que es éste el término que utiliza el RGPD, art. 4.5, frente al de pseudoanonimizados, presente en nuestro ordenamiento jurídico desde 2007: LIB, art. 3, k.

[76] Al mismo resultado llegaba su Reglamento, pero dando un cierto circunloquio de dudosa justificación: "procedimiento de disociación: todo tratamiento de datos personales que permita la obtención de datos disociados (art. 5.1, p); dato disociado es aquél que no permite la identificación de un afectado o interesado (art. 5.2, e) y estos últimos son la persona física titular de los datos que sean objeto del tratamiento (art. 5.1, a).

[77] Art. 3, i): "Dato anonimizado o irreversiblemente disociado: dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados. Art.3, k) "Dato codificado o reversiblemente disociado: dato no asociado a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa".

doble codificación, etc.), por lo general apoyados por técnicas digitales, pero en cualquier caso han de dar lugar a la separación de los datos identificadores de la persona del resto de la información que le concierna.

Más relevante es tener presente que la disociación puede ser reversible o irreversible, en los términos que expuse más arriba.

El concepto de disociación que acoge el RGPD parece ser el de disociación reversible, pues se requiere que "siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable", vimos que señala el art. 4.5 del RGPD.

Los procedimientos de disociación mediante el uso de técnicas de cifrado o codificación se utilizan con el fin, precisamente, de conferir una mejor protección a los datos, en especial cuando van a ser cedidos a terceros. Mientras éstos últimos no tengan acceso a esa información adicional separada puede afirmarse que nos encontramos ante datos de persona no identificable, al menos para los terceros a los que se les ceden o tienen acceso legítimo a los mismos. Sin embargo, no quedan completamente al margen del marco tutelar de la legislación de protección de datos; al contrario, continúan siendo objeto de protección legal, en concreto de acuerdo con los criterios que veremos que impone la legislación interna (LOPDGDD).

Esta es una matización o aclaración relevante a la que ha dado cabida explícita el RGPD: "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o *identificable*. *Los datos personales seudonimizados*, que cabría atribuir a una persona física mediante la utilización de información adicional, *deben considerarse información sobre una persona física identificable*"[78].

La disociación en cuanto tal no prejuzgaría la categoría jurídica de los datos que han sido sometidos a tal procedimiento: tanto pueden ser datos de personas identificables como no identificables (datos anónimos). Pero la respuesta sobre a qué categoría de datos pertenecen se debe buscar en, como se expuso en otro lugar, si requieren o no procedimientos no razonables o esfuerzos desproporcionados para lograr la identificación de la persona. Sin embargo, teniendo en cuenta los procedimientos de seudonimización que se utilizan habitualmente, esto es, la codificación de los mismos, en la

[78] RGPD cndo. 26.

mayor parte de los casos se tratará de datos de personas identificables y no de datos anónimos, sin perjuicio de que pueden utilizarse procedimientos de doble codificación u otros de semejante alcance que producen este último efecto. En consecuencia, estos datos estarán sometidos frecuentemente a los principios y al régimen legal de protección de los datos personales.

Si el procedimiento fuera irreversible entraríamos en la categoría de la anonimización.

5.3.4. Los derechos de la persona afectada sobre el proceso de anonimización y de seudonimización: alcance del consentimiento y del derecho a la información

Aparte de otras situaciones que abren la posibilidad de un tratamiento lícito de datos personales, el eje de esta licitud continúa asentándose en el consentimiento del titular de los datos –el interesado– para uno o varios fines específicos:

> "[El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:] el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos"[79].

Se ha discutido si el proceso mismo de anonimización requiere o no el consentimiento previo de la persona afectada o si es necesario al menos que sea informada sobre dicho proceso, también previamente, como hemos planteado más arriba. La misma cuestión se plantea cuando se pretende realizar la seudonimización. Mientras estos procesos se culminan o, incluso antes de que se inicien, nos encontramos ante verdaderos datos de carácter personal, esto es, atribuibles a un apersona identificada o identificable, por lo que no cabe duda de que su tratamiento requiere también para que sea legítimo, el consentimiento del interesado, a salvo de situaciones específicas que contemple la norma.

A favor de la exigibilidad normativa del cumplimiento de esta obligación puede alegarse el propio RGPD, en particular la amplia definición que aporta sobre "tratamiento", puesto que en ella se incluyen expresiones como

[79] RGPD art. 6.1, a. También el consentimiento es objeto de acotamiento definitorio por parte del RGPD: "Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (art. 4.11).

"adaptación", "modificación", o "limitación" de los datos, que es uno de los efectos más evidentes que comporta:

> "«Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"[80].

No cabe duda de que el sentido literal de este párrafo incluye las operaciones de anonimización –y de seudonimización–, en concreto como actividad de adaptación o modificación de los datos, dado que lo datos personales son sometidos a una alteración o mutilación con el fin de que no pueda identificarse a la persona de la que provienen aquéllos. El proceso mismo de anonimización comporta todavía un acto de tratamiento de datos personales. Significa esto que hasta que no se haya producido la anonimización de los datos personales éstos gozan de la consideración de tales y les es aplicable el régimen legal de protección de los datos.

Por otro lado, el mismo Reglamento establece claramente el derecho del interesado a prestar su consentimiento para la investigación con sus datos, reconociéndole la facultad de delimitar o restringir los fines de investigación sobre los que consiente: "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida"[81].

---

[80] RGPD art. 4.2.

[81] RGPD, cndo. 33. No obstante, no parece sencillo interpretar la relación de este considerando con el cndo. 50, que entiende que "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" y, en tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales; estimando explícitamente compatibles los fines de investigación científica. Pero a continuación marca limitaciones y condiciones cuyo alcance, dentro del mismo considerando, no es fácil de especificar, como ésta: "Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento

Por consiguiente, en algún momento antes de proceder a la anonimización o seudonimización (incluso aunque no se vayan a someter los datos a alguno de estos procesos) el interesado deberá expresar su consentimiento y el alcance del mismo y, como precisa el texto transcrito, es posible que no pueda prestarse aquél en el momento mismo de la recogida de los datos, lo que implica reconocer que puede ser en un momento posterior.

Se ha criticado esta solución por algún sector, pues se entiende que constituiría una exigencia imposible de llevar a la práctica, por las extraordinarias dificultades que puede comportar en muchos casos. Para otros, lo anómalo radicaba en los propios planteamientos de la anterior LOPD, que, se dice, eran incoherentes y contradictorios, dado que, por un lado, promovía la protección de la intimidad y animaba específicamente al uso de datos anónimos, pero, por otro, incluía el acto de la anonimización en su definición de 'tratamiento', de modo que ocluía la posibilidad de anonimización sin un consentimiento explícito por parte del interesado.

También se ha sostenido, en sentido contrario a la anterior posición, que la anonimización (con o sin procedimientos de agregación) no desplaza el deber de confidencialidad en relación con los sujetos de los datos. El fundamento de esta posición se encuentra en el riesgo de identificación de la persona a pesar de la anonimización. En resumen, el consentimiento continúa siendo la regla básica cuando se pretende revelar una información dada en una relación de confianza (p. ej., el llamado confidente necesario en el ámbito profesional o laboral).

En conclusión, puede confirmarse que, puesto que la anonimización comporta el tratamiento de datos personales, goza del estatuto jurídico que a éstos se reconoce en tanto no se haya culminado aquel proceso. En consecuencia, la persona titular de los datos no sólo debe ser consultada para que otorgue su consentimiento a la anonimización, sino que, además, está legitimada para rechazarla si, por ejemplo, no está de acuerdo con el uso o destino que vaya a darse a sus datos, de lo que se deriva que deberá ser informado previamente sobre este particular. Esta conclusión parece la

---

no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto." V. sobre este considerando Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, *op. cit.*

más coherente con los propósitos del régimen de protección de datos y ha encontrado un reflejo legal explícito en la LIB[82].

A semejantes reflexiones hemos llegado con anterioridad con respecto al procedimiento de codificación de los datos que comporten una mera disociación reversible de los datos identificadores (seudonimización), teniendo en cuenta que estos datos caen, en principio, bajo el régimen de protección legal, pues conciernen a personas identificables. El RGPD encomienda al responsable del tratamiento de los datos la seudonimización cuando, de acuerdo a determinados criterios técnicos, organizativos y otros similares, pueda realizarse para aplicar de forma efectiva los principios de protección de datos[83]. No es muy clara su dicción a la hora de establecer si para tomar esta decisión el responsable del tratamiento necesita o no el consentimiento del interesado. En todo caso, prevalece la normativa interna estatal, a la vista de las amplias facultades que reconoce el Reglamento a los EM en este ámbito[84].

Como es sabido, el recurso a los procedimientos de disociación de los datos es frecuente en los ámbitos estadísticos y de la investigación científica, en concreto en el sector de la Biomedicina. Esta alternativa de la disociación suele ser considerada como la deseable en relación con estas actividades: en ellas sólo interesan datos globales (estudios estadísticos y epidemiológicos), bien porque no se vaya a necesitar ninguna otra información de la persona que participa en la investigación, para lo que es suficiente con una disociación irreversible o anonimización, lo que tiene como efecto que libera al investigador de cualquier obligación ulterior respecto al tratamiento de los datos; o bien porque se cuente con la posibilidad de tener que solicitar más información al interesado para poder proseguir la investigación (p. ej., datos retrospectivos de la historia clínica relativos a la evolución de la enfermedad que padece que está siendo objeto de estudio) o, al contrario, porque se haya obtenido un hallazgo de capital importancia sobre la salud del interesado,

---

82 En concreto, en relación con las muestras biológicas: "El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización" (art. 58.2); "En el caso de utilización de muestras que vayan a ser anonimizadas, el sujeto fuente recibirá la información contenida en los apartados a), b), c) y d) de este artículo" (art. 59.2). Baste con citar la letra a) para comprender el alcance de la información previa a la anonimización: "Finalidad de la investigación o línea de investigación para la cual consiente" (art. 59.1, a).

83 RGPD, art. 25.1.

84 RGPD, art. 89.

que debe comunicársele con urgencia (p. ej., que es portador de una grave enfermedad que requiere tratamiento médico inmediato).

En estos casos puede ser conveniente proceder a una disociación reversible de los datos o seudonimización, para el caso en que sea necesario volver a ponerse en contacto con el interesado.

Además, debe recordarse lo ya señalado de que en el sector de la investigación científica el titular de los datos –el interesado– frecuentemente lo es no sólo de éstos, sino también de aquellos materiales biológicos (muestras biológicas)[85] de los que se puede extraer alguna información individualizada mediante las pruebas oportunas. Las muestras biológicas son tratadas por la LIB, con acierto, como material continente de información relativa al sujeto del que proviene y de su familia biológica, y por ello también les otorga protección. Esta ley confiere a las muestras biológicas el mismo régimen jurídico que a los datos personales relativos a la salud, y prevé para ellas la posibilidad tanto de su seudonimización como de su anonimización[86].

Por su parte, el *Information Commissioner* del Reino Unido[87] detectó con acierto hace ya unos años algunas dificultades planteadas por los datos anonimizados o, mejor, por el proceso que conduce a ellos: la eliminación del nombre y dirección no es suficiente para asegurar el anonimato, pues la identidad de una persona puede ser deducida de otros datos no eliminados, como la fecha de nacimiento y el código postal; un responsable de los datos no puede designar a un tercero para tratar datos en su representación y defender que, puesto que éste no visualiza la información personal en sí misma, no está "tratando" datos; tal argumento, se explica, no es aceptable,

---

[85] La LIB define el sujeto fuente como "individuo vivo, cualquiera que sea su estado de salud, o fallecido del que proviene la muestra biológica" (art. 3, v); y la muestra biológica: "cualquier material biológico de origen humano susceptible de conservación y que pueda albergar información sobre la dotación genética característica de una persona" (art. 3, o).

[86] Lo que explica que haya sido tan minuciosa en sus definiciones relativas a la situación de la muestra: "Muestra biológica anonimizada o irreversiblemente disociada: muestra que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable. Muestra biológica no identificable o anónima: muestra recogida sin un nexo con una persona identificada o identificable de la que, consiguientemente, no se conoce la procedencia y es imposible trazar el origen. Muestra biológica codificada o reversiblemente disociada: muestra no asociada a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa" (art. 3, p, q, r, respectivamente).

[87] Information Commissioner of the United Kingdom: *Guidance*, January 2001.

puesto que el responsable de los datos lo es también de la información que sea tratada por el sistema de procesamiento digital.

Las llamadas enfermedades raras plantean asimismo sus propios problemas. Puede ocurrir que no sea posible anonimizar la información relativa a un paciente que padece una enfermedad extremadamente rara, por tanto, infrecuente y por ello fácilmente identificable su singular portador.

Por otro lado, debemos retomar los otros intereses legítimos que pueden estar implicados en la anonimización y el uso posterior de estos datos, como es la investigación científica.

Algunas instituciones científicas británicas elaboraron un documento muy clarificador sobre esta cuestión[88]. En dicho documento hay un capítulo dedicado específicamente a "confidencialidad, seudonimización y anonimización", cuyas orientaciones son muy similares a las propuestas más arriba. Procede destacar ahora únicamente que cuando se prevé la posibilidad de hallar alguna información relevante para el sujeto fuente (p. ej., que es portador de una enfermedad) dichos resultados puedan ser comunicados por el equipo investigador al médico responsable de aquél, para lo que el proceso de seudonimización es más conveniente, pero no en las demás hipótesis.

Otro supuesto en los que está prevista la disociación obligada de los datos es el relativo a la conservación de los datos una vez cumplido el plazo establecido para la cancelación de los mismos y para otras medidas precautorias, sin perjuicio de la obligación de bloqueo.

5.3.5. Seudonimización y cesión de datos para investigación en biomedicina: su exclusión del régimen general sobre protección de datos

Una de las consecuencias prácticas más relevantes en relación con los procedimientos de la seudonimización de los datos, sean o no sean aquellos reversibles es, en primer lugar, la posibilidad de utilización de datos de personas identificables con fines de investigación científica, con el fin de que desde un punto de vista metodológico dicha investigación pueda aprobar resultados científicamente validables. De este modo, en muchas ocasiones no

[88] Royal Brompton & Harefield NHS Trust and National Heart & Lung Institute Ethics Committee, *Advice to investigators on specific problems in preparing applications for Ethical Review of Research Studies*, últ. revisión de 2009, *passim.*

será necesario acceder a datos de personas identificadas y de serlo, en todo caso, deberá estar justificado por razón de la propia naturaleza del estudio[89].

En ocasiones, las propias características de una investigación biomédica determinada pueden requerir que esté plenamente identificado el paciente del que provienen las muestras, así como su propia historia clínica, la cual puede ser imprescindible para conocer la evolución de la patología que presente aquél. Esta metodología de la investigación plantea la necesidad de aportar algunos criterios específicos dirigidos al logro de una eficaz protección de los datos y de la intimidad de la persona afectada. Desde la perspectiva del investigador, monitor y promotor aquéllos se basarán, fundamentalmente, en el tratamiento confidencial tanto de la muestra como de la información personal que se pueda obtener o de la que ya se disponga (p. ej., la historia clínica), así como en el deber de secreto por parte de los profesionales implicados y respecto al interesado contar con su consentimiento previo[90].

De acuerdo con las prácticas más extendidas en la actualidad, la investigación científica en este sector se realiza mediante la colaboración de varios grupos de investigación situados en centros, ciudades e incluso países diferentes, en no pocas ocasiones algunos de ellos no pertenecen a la UE, por lo que cobra capital interés la posibilidad de compartir y transferir datos y muestras biológicas de las personas que participan en la investigación (sujetos fuente). De ahí que sea decisivo el régimen jurídico de la cesión de los datos.

Esta materia de la comunicación –cesión– de datos estaba prevista en la LOPD. De conformidad con la misma, los datos de carácter personal objeto del tratamiento sólo podían ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. Aparte de varias excepciones que establecía a continuación de esta regla general, en relación con la cesión de datos disociados esta Ley señalaba lo siguiente:

---

[89] La Recomendación del Consejo de Europa sobre Protección de datos médicos da preferencia a que los datos médicos que se utilicen con fines de investigación científica sean anónimos: "Siempre que ello sea posible, los datos médicos utilizados para fines de investigación científica deberán ser anónimos. Las organizaciones profesionales y científicas, así como las autoridades públicas promoverán el desarrollo de técnicas y procedimientos que aseguren el anonimato" (principio 12.1).

[90] De nuevo la Recomendación citada señala algunos requisitos (principio 12.2). La LIB también marca los suyos propios, e incluye la hipótesis de que no pueda recabarse el consentimiento del sujeto fuente de la muestra biológica, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de la Ley (art. 58.2 y disposición transitoria segunda).

"Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores" (art. 11.6). El concepto legal de disociación en este precepto no quedaba muy claro: si se refería a la que conducía a la anonimización o a la mera seudonimización.

A diferencia de la perplejidad que generaba el régimen legal anterior, con la regulación actual se despeja esta incertidumbre, al considerar, como se indicó más arriba, que la disociación conducente a una seudonimización da lugar a que ésta no entre en el ámbito normativo respecto a la cesión de datos a terceros.

De todos modos, el temor persiste respecto a los riesgos de reidentificación, respecto a la cual el legislador interno ha establecido varios requerimientos.

6. La reidentificación y los requisitos de cesión de datos

6.1. El big data y los riesgos de reidentificación de los datos anonimizados o seudonimizados

La posibilidad real de reidentificación del titular de los datos, acrecentada con el tratamiento creciente del *big data*, supone el debilitamiento de un mecanismo adoptado jurídicamente sobre el que ha descansado en gran medida la cesión de datos a terceros ajenos a los fines legítimos perseguidos con su obtención[91], además del consentimiento del interesado y sus derechos de exclusión de terceros[92]: la anonimización, que, como se ha visto más arriba, comporta que los datos personales que han sido sometidos a este proceso de desidentificación aparentemente irreversible dejan de constituir un objeto de la protección y del régimen jurídico de los datos, puesto que han dejado de ser de carácter personal desde el momento en que se disgregan o separan definitivamente los datos identificadores de la persona del resto de datos que se refieren a ella.

Sin perjuicio de la realidad acabada de mencionar, al legislador interno lo que le preocupa es que la reidentificación pueda producirse en relación con los datos seudonimizados, una vez hayan sido cedidos a terceros para

[91] Así lo entienden también, Maye-Schönberger, V. / Cukier, K., *Big data. La revolución de los datos masivos*, Turner-Noema, 2013, p. 194.
[92] V. arts. 3 y 5 de la LIB.

investigación biomédica. Le preocupa y regula requerimientos que prevengan aquélla.

6.2. La prevención de la reidentificación

El legislador estatal, dada la iniciativa que hemos visto que otorga en esta materia el RGPD a los EM[93], no ha dudado en establecer la inclusión de medidas prescriptivas con el fin de prevenir lo mejor posible la reidentificación de datos seudonimizados. Distinto es que pueda aceptarse su propia formulación y compartir que estas medidas vayan a ser eficaces. Veámoslo.

Para el uso de datos personales seudonimizados se requerirá, según prescribe con mayor exactitud la LOPDGDD[94]:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. No podemos entrar más allá en esta exigencia, pero apunta a que el investigador y la persona que proceda a la seudonimización han de ser distintos. Este proceder es el estándar en relación con los biobancos, pero en otros ámbitos, como el hospitalario, puede ser más complicado observarlo, por ejemplo, cuando se trata de datos y muestras que proceden de pacientes del propio investigador.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación, ii) se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

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

Con esta última previsión deberá armonizarse lo establecido por la LIB sobre este mismo asunto (aunque está redactado con matices diferentes de cierta relevancia, en los que no podemos entrar en este lugar), conforme

93 Recuérdese lo que establece el RGPD en su art. 89.
94 Disposición Adicional 17.2, d), párr. 2º LO 3/2018.

a la cual antes de realizarse un análisis genético con fines de investigación en el ámbito sanitario deberá informarse al interesado de: la posibilidad de descubrimientos inesperados y su posible trascendencia para el interesado; la facultad de éste de tomar una posición en relación con recibir su comunicación; y la implicación que puede tener para sus familiares la información que se llegue a obtener y la conveniencia de que él mismo, en su caso, transmita dicha información a aquéllos (art. 47, nºs 4º y 5º).

Es indudable que la reidentificación de los datos, buscada o accidental, es uno de los grandes desafíos a los que se enfrentan la normativa europea (RGPD) y la interna (LOPDDGDD) para asegurar su eficiencia; pero es al mismo tiempo es su talón de Aquiles. Las medidas legales que se han adoptado (exclusivamente centradas en el sector de la salud en lo que se refiere a la legislación interna; nada explícito se indica en la europea) son más bien voluntaristas, al menos en parte, y todo parece presagiar que esta cuestión será la que desencadene en primer lugar las dudas sobre la eficiencia protectora del nuevo marco legal europeo y su desarrollo por las legislaciones internas de los Estados Miembros.

El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica, deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial[95].

7. Consideraciones finales. Algunas propuestas

El RGPD comporta un gran paso para una protección de los datos de carácter personal en general, incluidos los relativos a la salud y los genéticos. No obstante, es necesaria una protección más efectiva de estos datos, pues ya se ha visto la gran presión que se ha despertado en torno a ellos, en concreto respecto a su acceso por entidades del sector privado, en particular del sector productivo y financiero, pero también de las autoridades administrativas y sus agentes y de los propios ciudadanos como individuos.

Nadie se salva. Esto se agrava por el riesgo de reidentificación de los datos seudonimizados, pues la impresión es que las medidas preventivas que establece la LOPDPGDD no parecen suficientemente eficaces.

[95] Disposición Adicional 17.2, g), LO 3/2018, donde se añade que, en defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

Se debería prestar atención a las debilidades conocidas en la gestión de los datos de salud y genéticos y preparar algunas disposiciones específicas adecuadas para prevenir estos fallos en la protección de los datos sanitarios.

Medidas que podrían adoptarse o asegurar su eficiente ejecución si ya están incluidas en el RGPD o en la legislación interna (LOPDGDD):

- Prevenir el cruce de datos genéticos identificados con otros datos después de su anonimización.

- Reforzar y extender los deberes de confidencialidad de cualquier persona que gestione o acceda legítimamente a datos personales y agravar las consecuencias jurídicas en el caso de su vulneración, no solo personales, sino también institucionales[96]

- La multa no debería ser la principal o única respuesta.

- Implementar una aplicación real y eficiente del principio de minimización de los datos[97].

- Asegurar que el consentimiento del interesado sea prestado de forma verdaderamente libre, sin condiciones o requerimientos que coaccionen la libertad de la decisión del sujeto.

La panoplia de soluciones posibles es amplia. Tal vez podría ser suficiente con establecer legalmente un repertorio extenso pero flexible de garantías y obligaciones cuando los datos se utilizan para ciertos propósitos, más que recurrir a numerosas autorizaciones y consentimientos, p. ej., para la investigación en Biomedicina.

En esta inquietud de lograr una regulación lo más eficiente posible, algunas propuestas se dirigen a situaciones más definidas, bien que propugnando

[96] Sobre este particular el Derecho español establece esta obligación de forma adecuada: LIB, art. 5.4: "Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación". Código Penal, art. 197 y ss. (espec. 197.2 y 199).

[97] V. RGPD, arts. 5.1, c ("Los datos serán: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados") y 25. Entiende que se extiende a las garantías que establece el art. 89.1, Nicolás Jiménez, Pilar, *Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de Investigación biomédica*, *op. cit.*

criterios más limitados, pero al mismo tiempo más eficaces, como sería prestar más atención a la fase de recogida de datos para su posterior procesamiento, introduciendo mayores restricciones en esta actividad, pues es evidente la gran voracidad que se ha ido extendiendo de forma general respecto a la recogida de datos y su registro, lo que pone en duda que se cumpla la estricta observancia del principio de pertinencia o de proporcionalidad de la misma en relación con la finalidad legítima perseguida. La autonomía del titular de los datos podría expresarse una vez conocida su existencia y tomar a partir de ese momento las decisiones que aquél estime oportunas, sin perjuicio de las limitaciones u otras previsiones que haya podido establecer la ley.

También se apunta la necesidad de reforzar los deberes de confidencialidad de cualquier persona que gestione o acceda legítimamente a datos personales, aunque sobre este particular el Derecho español establece esta obligación de forma adecuada[98].

Probablemente debería abordarse un nuevo enfoque sobre los derechos de autonomía del interesado o titular de los datos, podría ser un control más eficiente por parte de las autoridades competentes del uso de los datos por parte de terceros, es decir, de su cesión, una vez otorgado el consentimiento inicial por aquél.

[98] LIB, art. 5.4: "Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación."

Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos*

Rights over data used for biomedical research purposes in new technological and scientific scenarios

Profa. Dra. Pilar Nicolás

Investigadora doctora permanente, Departamento de Derecho Público, Facultad de Derecho de la Universidad del País Vasco UPV/EHU

Grupo de Investigación Cátedra de Derecho y Genoma Humano de la Universidad del País Vasco UPV/EHU (Bilbao, España)

DOI: 10.14679/1135

Sumario / Summary: 1. Introducción. 2. El nuevo marco jurídico. 2.1. Panorama general. 2.2. El sujeto titular de los datos. 3. Derecho de oposición y derecho a la limitación del tratamiento. 3.1. Cuestiones generales. 3.2. Limitaciones y excepciones. 4. El derecho de acceso a los datos personales almacenados. 4.1. El objeto del derecho 4.2. La obligación de hacer efectivo el derecho. 4.3. Acceso a

* Artículo recibido el 20 de agosto de 2019 y aceptado para su publicación el 18 de septiembre de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos -*Big Data*-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER)".

La investigadora pertenece al Grupo de Investigación Catedra de Derecho y Genoma Humano, Grupo de Investigación del Sistema Universitario Vasco (IT 1066-16).

datos de fallecidos. 4.4. Limitaciones y excepciones. 5. El derecho a la supresión de los datos. 5.1. Principios relativos al tratamiento de datos y derecho a la supresión. 5.2. Supresión de datos de fallecidos. 5.3. Limitaciones y excepciones. 6. Derecho a la rectificación. 7. El derecho a ser informado de los datos relevantes para la salud. 7.1. La base jurídica del derecho. 7.2. Mecanismos de garantía. 7.3. Limitaciones y excepciones. 8. El derecho a conocer los resultados globales de la investigación. 9. Conclusión. 10. Bibliografía.

Resumen / Abstract: La utilización y combinación de grandes volúmenes de datos representan, también el ámbito de la biomedicina, oportunidades para la generación de conocimiento, para la solución de problemas y para mejorar las condiciones de vida de las personas. No obstante, reconocer las ventajas y las oportunidades que las nuevas tecnologías ofrecen ha de implicar, a la vez, una previsión y evaluación de las consecuencias que este nuevo escenario puede acarrear para los derechos de los individuos, si es que no se enmarca en unas garantías adecuadas. El RGPD Reglamento y la normativa española de desarrollo reconocen distintas bases jurídicas, junto con el consentimiento del sujeto, para tratar los datos de carácter personal relativos a la salud y los datos genéticos, en particular cuando se trata de finalidad científica. Es importante subrayar que estas otras bases jurídicas no podrán sustentar el tratamiento si suponen que las garantías para los derechos de los titulares quedan debilitadas. Esta condición exige que los derechos del titular sobre sus datos estén nítidamente definidos y protegidos, lo que puede incluso significar un mecanismo que otorgue un control más reforzado que la expresión de un consentimiento.

The use and combination of large volumes of data represent, also in the field of biomedicine, opportunities for the generation of knowledge, for the solution of problems and to improve people's living conditions. However, recognising the advantages and opportunities offered by new technologies must involve both forecasting and evaluating the consequences that this new scenario may have for the rights of individuals, if it is not framed within adequate guarantees. The GDPR and the Spanish implementing legislation recognize different legal bases, together with the consent of the subject, for processing personal data relating to health and genetic data, particularly when it is for scientific purposes. It is important to underline that these other legal bases will not be able to sustain the treatment if they suppose that the guarantees for the rights of the holders are weakened. This condition requires that the rights of the data subject over his data are clearly defined and protected, which may even mean a mechanism that gives a stronger control than the expression of consent.

Palabras clave / Keywords:

Protección de datos / Investigación biomédica / Derechos sobre los datos / *Bigdata.*

Data protection / Biomedical research / Rights over the data / Bigdata.

1. Introducción

La acumulación de grandes volúmenes de datos en sistemas informáticos y las nuevas herramientas tecnológicas para su análisis (*bigdata*)[1] representan, también el ámbito de la biomedicina, oportunidades para la generación de conocimiento, para la solución de problemas y para mejorar las condiciones de vida de las personas, tal como queda reflejado en el considerando 157 del Reglamento general de protección de datos –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 (RGPD)–. Este considerando reconoce que la combinación de información procedente de diferentes y grandes registros, facilita la adquisición de un conocimiento muy valioso sobre la salud y la enfermedad, puesto que estará basado en un volumen mayor de información[2].

Por otra parte, las inversiones en recursos humanos, organizativos, tecnológicos, y en infraestructuras, imprescindibles para generar y almacenar esta información, serán más provechosas cuantos más usuarios (profesionales de la biomedicina) puedan beneficiarse de su uso, ya sea primario (como propósito fundamental que las justificó) o secundario. La historia clínica electrónica es un recurso muy valioso en este sentido, puesto que constituye un enorme repositorio de información de un elevado número de personas, si bien su adaptación a las necesidades de la investigación requiere un importante esfuerzo técnico y humano.

---

[1] El término *bigdata* hace referencia "al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo", Agencia Española de Protección de Datos, *Código de buenas prácticas en protección de datos para proyectos big data*, 2018, p. 3.
Sobre el fenómeno del *bigdata* en la investigación epidemiológica, véase el informe de la Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, Barcelona, España, Noviembre de 2017, pp. 30 y ss.

[2] "Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales".

No obstante, reconocer las ventajas y las oportunidades que las nuevas tecnologías ofrecen ha de implicar, a la vez, una previsión y evaluación de las consecuencias que este nuevo escenario puede acarrear para los derechos de los individuos, si es que no se enmarca en unas garantías adecuadas. Téngase en cuenta, además, que el tratamiento de los datos supondrá no sólo gestionar la información existente (en procesos conocidos con mayor o menor detalle por los sujetos) sino, además, generar nuevos datos, esto es, nueva información sobre aspectos sensibles para la vida de las personas (salud o relaciones de parentesco) desconocida para los propios sujetos.

La aplicación de estas nuevas herramientas no sería operativa en un marco normativo rígido basado en el consentimiento expreso y escrito como condición para el tratamiento de datos de salud y paradigma de las garantías de los procesos, o que abordase las categorías jurídicas de una manera estática y no dinámica o cambiante. Por eso, el nuevo modelo de protección que implanta el RGPD, fundamentado en unos principios generales y desarrollado a través de garantías que deben ser diseñadas para cada modelo de tratamiento, es satisfactorio a estos efectos[3].

Por ejemplo, el Reglamento y la normativa española de desarrollo reconoce otras bases jurídicas, distintas al consentimiento, para tratar los datos de carácter personal relativos a la salud y los datos genéticos, en particular cuando se trata de finalidad científica. Es importante subrayar que estas otras bases jurídicas no podrán sustentar el tratamiento si suponen que las garantías para los derechos de los titulares quedan debilitadas. Esta condición exige que los derechos del titular sobre sus datos estén nítidamente definidos y protegidos, lo que puede incluso significar un mecanismo que otorgue un control más reforzado que la expresión de un consentimiento.

En el marco de la investigación biomédica, no se debe olvidar que nuestro ordenamiento jurídico incorporó el principio de primacía del ser humano en el año 2000, con la entrada en vigor del Convenio de Biomedicina del Consejo de Europa, y que ha plasmado en el artículo 3 de la Declaración de

[3] Se ha afirmado que el RGPD afronta esta material desde un "research-friendly approach" y que "According to the Regulation, using data for research purposes and sharing it for downstream uses require adopting further organizational safeguards, which go beyond the consent or anonymization approaches. Nevertheless, the Regulation does not elaborate further on such safeguards, leaving it primarily to the Member States to adopt adequate safeguards and conditions for processing data under the research exemption". Shabani, Mahsa / Borry, Pascal, "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation", *European Journal of Human Genetics*, Núm. 26, 2018, p. 154.

Bioética de la UNESCO, de 2005 y está recogido en la Ley 14/2007, de 3 de julio, de Investigación Biomédica (LIB): "la salud, el interés y el bienestar del ser humano que participe en una investigación biomédica prevalecerán por encima del interés de la sociedad o de la ciencia". El irrenunciable respeto al principio de primacía del ser humano supone que la protección de los derechos de las personas y, por lo que aquí interesa, de los derechos a la intimidad y a la autodeterminación informativa, prevalece sobre el interés exclusivo del progreso científico o de otros intereses colectivos.

Es importante señalar que el derecho a la autodeterminación informativa en el ámbito sanitario se entiende en el proceso de evolución desde una relación paternalista entre el profesional y el sujeto o paciente, hacia otra en la que es la persona decide sobre los procesos que le atañen porque conoce las circunstancias en las que se encuentra. Como señala el artículo 5 de la Declaración de Bioética de la UNESCO: "Se habrá de respetar la autonomía de la persona en lo que se refiere a la facultad de adoptar decisiones, asumiendo la responsabilidad de éstas y respetando la autonomía de los demás. Para las personas que carecen de la capacidad de ejercer su autonomía, se habrán de tomar medidas especiales para proteger sus derechos e intereses".

Este punto de partida sitúa los intereses de los individuos por encima de los más abstractos intereses colectivos, pero no significa que éstos se vayan a obstaculizar o perjudicar si es que se implantan mecanismos que supongan garantías para aquellos. Así, por ejemplo, un comité de ética podría avalar la utilización de datos o muestras de pacientes sin consentimiento para un estudio de interés científico cuando éstos no tuvieran acceso a los identificadores y no se apreciase un riesgo para los derechos de estas personas.

En este marco, el ordenamiento jurídico ha articulado un sistema de garantías para la protección de los sujetos que participan en investigación científica en el que se incluyen ciertos derechos en relación con los datos obtenidos a partir de intervenciones invasivas, del análisis de muestras biológicas o de otros archivos y registros, y que son una manifestación del reconocimiento del individuo como verdadero sujeto de la investigación, con facultades para controlar la información que se genera gracias a su participación, más allá del consentimiento inicial, que es previo al archivo de los datos. Viene al caso recordar la STC 292/2000, de 30 de noviembre, que resumió el contenido del derecho a la autodeterminación informativa en los siguientes términos "el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos […] que sirven a la capital función que

desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (FJ 6º).

Al hilo de este planteamiento, viene al caso subrayar que la configuración de los derechos sobre los datos en nuestro ordenamiento jurídico no puede ser abordada desde una perspectiva patrimonial. Los datos de carácter personal constituyen un bien de la personalidad y los derechos que se ostentan en relación con su tratamiento no tienen aquella naturaleza. El titular de los datos será siempre el sujeto identificado o identificable a partir de esa información, que mantiene el control (y las correspondientes facultades que emanan de ese poder jurídico) mientras dure el tratamiento. Esto no significa que puedan existir, además, otros derechos sobre los datos, derivados, por ejemplo, de la inversión en su generación o almacenamiento[4]. Estos derechos podrán llegar a limitar, pero no eliminar las facultades del sujeto titular del derecho a la autodeterminación informativa, que subsiste mientras la información revista carácter personal.

2. El nuevo marco jurídico

2.1. Panorama general

Un instrumento legislativo supranacional para el tratamiento de datos en el área de la biomedicina facilita operaciones que trascienden las fronteras nacionales (asistencia sanitaria transfronteriza, disponibilidad de información validada para facilitar diagnósticos, investigación científica, cuestiones de salud pública, etc). Además, en el caso de la UE, resulta imprescindible para alcanzar los objetivos de la Unión en cuanto a la libertad de circulación de servicios y de personas.

La aprobación del RGPD supuso un cambio importante en la Unión Europea en materia de protección de datos con fines relacionados con la biomedicina (si bien no tanto en un ámbito estrictamente clínico). En comparación con la Directiva de 1995, el RGPD presta mucha más atención

[4] Gil, Elena, *Bigdata, Privacidad y protección de datos*, Agencia Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2016, p. 139.

a esta cuestión, y lo hace con un enfoque abierto a los nuevos escenarios tecnológicos, como ya se señaló.

No obstante, la naturaleza homogeneizadora del reglamento no se ha desplegado de forma efectiva en esta área, donde el margen de desarrollo normativo para los Estados se ha definido en términos muy amplios.[5]

La base del régimen reforzado para los datos de salud se sitúa en el artículo 9, que establece, como regla general, la prohibición del tratamiento de datos genéticos y de datos relativos a la salud salvo que concurra, entre otras, algunas de las siguientes circunstancias:

- Que el interesado haya prestado su consentimiento.
- Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.
- Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
- Que el tratamiento sea necesario por razones de un interés público esencial, para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.
- Que el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.

[5] En este sentido se ha llegado a afirmar que el Reglamento "perpetuates the fragmented approach to data protection in health research which had been a problem with the Data Protection Directive", Donnelly, Mary / Mcdonagh, Maeve, "Health Research, Consent and the GDPR Exemption", *European Journal of Health Law*, Núm. 2, Vol. 26, 2019, p. 98.

- Que el tratamiento sea necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

En todos los casos se requiere que concurra proporcionalidad entre la naturaleza y cantidad de los datos y la finalidad perseguida, que se implanten medidas específicas que garanticen los derechos de los sujetos, y, en algunos supuestos, que exista una base jurídica en derecho de la unión o de los Estados. Por otra parte, se prevé que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Por otra parte, ciertas medidas previstas a lo largo del RGPD, como la necesidad de llevar a cabo una evaluación de impacto (artículo 35) o de nombrar un delegado de protección de datos (artículo 37), serán de aplicación al tratamiento de datos en las áreas científica y sanitaria[6].

En particular, el Reglamento está salpicado de menciones al tratamiento con fines de investigación biomédica, como propósito que legitima el tratamiento de datos o justifica flexibilizar sus condiciones, con el trasfondo del artículo 89, que prevé como regla general la implementación de medidas adecuadas de garantía[7] y que está redactado en términos muy abiertos, dejando margen a la regulación de los Estados miembros.

Su entrada en vigor en España, en estos términos, no tuvo un impacto de calado inmediato, pero impulsó la articulación de un régimen global para la regulación del tratamiento de datos con fines de investigación científica, que no existía en nuestro ordenamiento jurídico[8].

Como es sabido, la opción legislativa para desarrollar las condiciones específicas del tratamiento de datos con fines de investigación biomédica

---

[6] Troncoso Reigada, Antonio, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano / Law and the Human Genome Review*, Núm. 49, 2018, p. 261.

[7] De hecho, como se ha afirmado, lo que actualmente se consideran buenas prácticas en la investigación cumpliría con esta exigencia. Dove, Edward, "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era", *The Journal of Law, Medicine & Ethics*, Núm. 4, Vol. 46, 2018, p. 8.

[8] Nicolas, Pilar, "Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de investigación biomédica", *Comentarios al Reglamento General de Protección de Datos y a Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*, Troncoso Reigada, Antonio (Dir), Thomsom Reuters Aranzadi, Cizur Menor, España, 2019, *passim*.

ha sido su integración en la normativa general (Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales –LOPDyGDD–): disposición adicional (DA) 17ª, a la que ahora se remite la Ley 14/1986, de 25 de abril, General de Sanidad en un nuevo capítulo –"Tratamiento de datos en la investigación en salud"–, de su Título VI (Disposición final quinta de la LOPDyGDD).

El nuevo escenario se asienta, básicamente, en dos pilares: primero, la legitimidad del tratamiento exige que el responsable implante medidas técnicas y organizativas adecuadas al contexto del tratamiento, lo cual va más allá de la exigencia de consentimiento expreso y específico del sujeto (el mecanismo "clásico" de garantía); y segundo, se impone la intervención de organismos independientes de revisión (Comités de Ética de la Investigación –CEI–) para verificar la legitimidad del tratamiento en cada supuesto concreto.

En las siguientes páginas se pretende analizar las facultades que el sujeto ostenta sobre los datos que se utilizan con fines de investigación, que emanan del derecho a la autodeterminación informativa (oposición, limitación, acceso, rectificación, supresión) o de otros títulos jurídicos, como el derecho a recibir información relevante para la salud y el derecho a conocer los resultados globales de la investigación.

2.2. El sujeto titular de los datos

El sujeto que ostenta este derecho es el interesado, el sujeto de la información, es decir la persona "cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (art. 4.1. RGPD).

Se ha afirmado que el carácter hereditario de los datos genéticos de la línea germinal, supone que el tratamiento se aborda desde una perspectiva supraindividual. De hecho, se suele denominar consejo genético familiar, al proceso en el cual se indican y practican los análisis y se transmite la información. No obstante, en el plano jurídico la familia no se constituye en una suerte de "paciente o sujeto colectivo" con potestad sobre los datos que se obtengan en del análisis. El sujeto del derecho a la autodeterminación informativa es el sujeto fuente de la muestra a partir de la cual se obtienen los datos. En esta línea, el RGPD define en el art. 4. 13 los "datos genéticos"

como "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Este punto de partida no significa que los intereses de terceros queden desatendidos cuando puedan estar implicados en el tratamiento de los datos: si bien los familiares del sujeto no son titulares de la información, lo cierto es que eventualmente la pueden compartir (cosa que no se sabe con certeza hasta que se les realicen a ellos los correspondientes análisis) y este hecho se tiene en cuenta en la articulación de soluciones de ciertos conflictos que pudieran surgir, pero sin que se justifique el reconocimiento de un correspondiente derecho sobre la información. Por ejemplo, cuando el titular opta por no conocer los resultados de un análisis pero estos pueden ser relevantes para la salud de sus familiares, se establecen vías para hacerles llegar a estos la información. Es el derecho a la protección de la salud y a la integridad física, y no el derecho de acceso a los propios datos, el título jurídico que justifica la comunicación de la información en estos casos[9].

Un asunto discutido en relación con la utilización de datos de menores o incapaces con fines de investigación biomédica es si es o no necesario contactar con el sujeto para solicitar que consienta por sí mismo al alcanzar la mayoría edad o la capacidad plena, especialmente cuando su almacenamiento se pueda prolongar durante largos periodos, incluso indefinidamente, en régimen de colección o biobanco. Esta discusión tiene también repercusión en relación con el ejercicio de los derechos sobre los datos almacenados. En efecto, a favor de aquella exigencia se sostiene que representa el único mecanismo para garantizar que el sujeto tendrá noticia de la donación y podrá ejercer por sí mismo estos derechos, que en el caso de datos genómicos tienen una especial relevancia por tratarse de información que puede revelar información inesperada y que podrá suponer riesgos más elevados de identificación del sujeto.

En contra, puede decirse que desde el punto de vista jurídico el consentimiento que prestaron los representantes legales en lugar del menor o incapaz sigue siendo válido alcanzada la mayoría de edad, que la obtención de muestras o datos no significa su efectiva utilización en una investigación y que, en todo caso, cuando se vayan a utilizar, un Comité de Ética deberá decidir en el supuesto concreto si es necesario el consentimiento específico

[9] Lapunzina, Pablo / Nicolás, Pilar (coords.), *Gestión de datos genómicos con finalidad clínica y de investigación*, Idemm Farma, Madrid, España, 2015. pp. 59 y 60.

del sujeto (artículo 32.2 del RD 1716/2011). En todo caso, el investigador o el responsable del biobanco deberán tener en cuenta la fecha en que el sujeto alcance la mayoría de edad a efectos de futuros contactos (p. ej., para informar sobre el cierre del biobanco, para comunicar un hallazgo relevante para la salud, etc.), y también de la disponibilidad de la información como se prevé en el artículo 32 (art. 32.3: "En el caso de utilización de muestras de menores de edad con fines de investigación biomédica, según lo previsto en el artículo 58.5 de la LIB, el biobanco y las personas responsables de la colección o del proyecto de investigación tendrán la información a la que se refiere el apartado 1 de este artículo a disposición de la persona representante legal del sujeto fuente hasta que este alcance la mayoría de edad, y del propio sujeto fuente a partir de ese momento").

Por otra parte, la normativa general sobre protección de datos (RGPD y LOPDyGDD) no exige contactar con quien que no prestó el consentimiento por sí mismo o no fue informado del tratamiento (porque fue sustituido en estos actos por sus representantes legales) cuando alcance la capacidad para consentir por sí mismo o entender la información correspondiente, para que subsista la base legal del tratamiento[10].

Conviene señalar que este planteamiento debe diferenciarse de la obligación de recabar el consentimiento del sujeto cuando adquiere la capacidad en el curso de la investigación, puesto que en este supuesto no se trata de un "recontacto", sino de la solicitud de consentimiento para continuar una investigación. Este es el sentido de la obligación que ha recogido el 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: "En el caso de menores o personas con la capacidad modificada y para dar su consentimiento, habiendo dado el consentimiento su representante legalmente designado, cuando estos alcancen o recuperen la capacidad de consentir, deberá recabarse su consentimiento para continuar participando en el ensayo clínico" (art. 4.3).

Sin embargo, lo cierto es que la primera de las posturas es mayoritaria entre los autores y ha sido recogida también en la Recomendación Rec (2016) 6 del Comité de Ministros del Consejo de Europa relativa a la investigación

[10] El Reglamento, sí hace hincapié en la relevancia del derecho al olvido para el caso en que el interesado hubiera dado su consentimiento siendo niño, sin ser plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet (Considerando 65) (…).

con muestras biológicas humanas establece que "*Where a person not able to consent, whose biological materials have been stored for future research, attains or regains the capacity to consent, reasonable efforts should be made to seek the consent of that person for continued storage and research use of his or her biological materials*" (art. 12.5). La repercusión de esta posición debería consensuarse para que no se genere inseguridad para los biobancos y los investigadores.

Finalmente, para cuestiones relativas al tratamiento de datos de fallecidos, véase lo señalado en los epígrafes 4.3 y 5.2.

3. Derecho a la oposición y derecho a la limitación del tratamiento

3.1. Cuestiones generales

Los derechos a la oposición y a la limitación tienen en común que suponen una manifestación de voluntad contraria al tratamiento de los datos.

El ejercicio del derecho a la oposición en el ámbito de la investigación biomédica adquiere mucha relevancia en un sistema que admite el tratamiento sin consentimiento expreso. Es el reflejo de la regla del llamado *opt ut*, según el cual, en determinadas condiciones se admite el tratamiento de datos sin consentimiento, siempre que se garantice que el sujeto pueda oponerse al tratamiento (como un sistema de presunción iuris tantum).

Está recogido en el artículo 21 del RGPD en los siguientes términos: "(…) 6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público".

El derecho a la oposición se ejerce antes o después del inicio del tratamiento. En el segundo caso está estrechamente relacionado con el derecho a la supresión.

El Derecho a la limitación tiene también como efecto el cese en el tratamiento, pero con carácter transitorio o parcial, por un determinado periodo de tiempo o con determinados fines. Está formulado en el artículo

18 del RGPF, según el cual "1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado".

La limitación del tratamiento supone "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro" (art. 4 RGPD). Los datos cuyo tratamiento queda limitado no se suprimen, sino que se conservan a diferentes efectos pero no se pueden utilizar ni ceder más allá de ese momento. Puede ejercerse cuando el mantenimiento es obligatorio o necesario pero el titular no desea una posterior utilización (tendría semejanzas con el derecho a la oposición al tratamiento) o cuando lo que se pretende limitar precisamente es la modificación o supresión (para una eventual presentación de reclamación o de prueba de un tratamiento ilícito).

La limitación se puede hacer efectiva a través de distintos procedimientos que consistan en "trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio de Internet" (considerando 67 RGPD).

3.2. Limitaciones y excepciones

Según el apartado 2 del art. 89, "Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los arts. 15, 16, 18 y 21", pero estas excepciones están sujetas a ciertas limitaciones, puesto que sólo se podrán prever si es que el ejercicio de los derechos pudiera implicar un obstáculo para el logro de los fines científicos y cuanto estas sean necesarias para alcanzar esos fines. (párrafo segundo del artículo 89). Estos artículos se refieren a los derechos de acceso, rectificación, limitación y oposición.

La DA 17ª de la LOPD y GDD ha recogido esta posibilidad en la letra e de su apartado 2 para tres supuestos: primero, cuando su ejercicio parece inviable porque se lleva a cabo ante quien no puede vincular los datos a la identidad del titular ("los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados"); segundo, cuando su ejercicio se refiera a datos o obtenidos en la investigación (lo cual podría justificar la excepción a otros derechos, pero no al de acceso en relación con datos de carácter personal) de justificar) y, tercero cuando su ejercicio pueda comprometer determinados intereses (seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley. No se debe olvidar que, como se advirtió, según el art. 89.2 RGPD, estas excepciones sólo se podrán invocar "cuando esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines".

Plantear excepciones al derecho a la oposición tiene importantes consecuencias para la autonomía de los sujetos puesto que implica que los datos se utilizan *contra* su voluntad. Justificar esta situación simplemente en el obstáculo que la oposición pueda representar para una investigación sería más o menos sencillo en cualquier supuesto en que dichos datos fueran interesantes para la investigación, lo que resulta claramente desproporcionado. Por eso, las excepciones a este derecho deberían estar sustentadas en la necesidad de remover un grave obstáculo para una investigación de un interés singularmente elevado. En este sentido, dice el art. 21.6 RGPD, que el derecho a la oposición al tratamiento con fines de investigación científica o histórica o fines estadísticos de conformidad con el art. 89, apartado 1", sólo podrá limitarse cuando dicho tratamiento "sea necesario para el cumplimiento de una misión realizada por razones de interés público". De una lectura sistemática de este precepto junto con el artículo 89.2, se puede concluir que las excepciones al derecho a la oposición tienen un tratamiento más restrictivo que las que puedan establecerse para el derecho de acceso, rectificación o limitación.

En cuanto al derecho a la limitación, en el marco de la investigación su ejercicio podría obstaculizar la continuidad de una investigación o la publicación de resultados en su primera faceta (limitación de la continuidad de su utilización) pero no parece que pueda ocurrir lo mismo si se solicita el mantenimiento de los datos.

4. El derecho de acceso a los datos personales almacenados

El derecho de acceso a los datos personales almacenados tiene un carácter instrumental muy relevante puesto que permite conocer qué datos están siendo objeto de tratamiento y hacer así efectivo el poder de control sobre la información personal. Por consiguiente, como se ha afirmado, "cuando el individuo pretenda el acceso a sus datos personales y a la información relativa a sus datos personales (incluidos datos personales de otros) con otras finalidades no está ejerciendo este derecho sino otro que el ordenamiento le pueda reconocer"[11]. Por esta razón, cuando el acceso esté justificado como mecanismo para proteger la salud del sujeto, quien lo ejerza lo hará en virtud de ese otro derecho, de naturaleza diferente, como veremos más adelante.

El derecho de acceso se recoge en el artículo 15 del RGPD, según el cual, el responsable del tratamiento, ante una solicitud del interesado, debe confirmar si sus datos están o no están siendo objeto de tratamiento y en qué condiciones (qué datos se están tratando, con qué finalidad, a quién se comunicarán y cuánto tiempo se van a conservan o qué criterio va a determinar este plazo). Este derecho subsiste durante todo el periodo de archivo de los datos como información personal, es decir, hasta su cancelación o anonimización.

El incumplimiento del deber de satisfacer el derecho de acceso es una infracción leve salvo cuando es reiterado, caso en que la infracción será grave o muy grave, según el nivel de identificabilidad del sujeto para quien deba satisfacerlo (artículos 74 c; 73 c; 72.1 k de la LOPDy GDD).

El derecho de acceso a los datos personales obtenidos en el curso de una investigación biomédica está reconocido en el Protocolo Adicional al Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa, relativo a la investigación biomédica, del año 2005[12] y en la LIB[13]; y con los

[11] Hernández Corchete, Juan Antonio, "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", Piñar, José Luis (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Ed. Reus, Madrid, España, 2017, p. 225.

[12] Artículo 26: "Right to information 1 Research participants shall be entitled to know any information collected on their health in conformity with the provisions of Article 10 of the Convention. 2 Other personal information collected for a research project will be accessible to them in conformity with the law on the protection of individuals with regard to processing of personal data".

[13] 49. 1: "El sujeto fuente será informado de los datos genéticos de carácter personal que se obtengan del análisis genético según los términos en que manifestó su voluntad,

datos genéticos en general en la Declaración Internacional sobre los datos genéticos humanos de la Unesco del año 2003 (art. 13)[14].

4.1. El objeto del derecho

El objeto de este derecho es cualquier dato de carácter personal que esté siendo objeto de tratamiento. Es decir, cualquier "información sobre una persona física identificada o identificable («el interesado»)" (artículo 4.1 del RGPD), lo que abarca "la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas" (considerando 35 RGPD). Por consiguiente, son datos de carácter personal a estos efectos los resultados de cualquier análisis o prueba si el sujeto es identificable, independientemente de su relevancia o de su interpretación en relación con la hipótesis científica planteada en el proyecto de investigación. Se incluyen en esta categoría, por ejemplo, datos genómicos crudos o variantes genéticas sin un significado clínico validado[15]. El derecho abarca tanto los datos que se recogieron para iniciar la investigación, como aquellos otros obtenidos a lo largo de la misma. Evidentemente, si los datos son objeto de un proceso de anonimización, ya no son información de carácter personal y, por consiguiente, tampoco objeto de este derecho. El sujeto debería ser informado de las previsiones que existan en este sentido.

También es objeto de este derecho la información sobre las cesiones de datos que se hayan llevado a cabo, tanto si se hubiera consentido expresamente a cada una de ellas como si no por no haber sido requerido el consentimiento específico a estos efectos por cualquier razón (por ejemplo, se encontraba englobado en el consentimiento inicial o el Comité de Ética

---

sin perjuicio del derecho de acceso reconocido en la legislación sobre protección de datos de carácter personal, que podrá suponer la revocación de la previa manifestación de voluntad libre otorgada".

[14] Nadie debería verse privado de acceso a sus propios datos genéticos o datos proteómicos, a menos que estén irreversiblemente disociados de la persona como fuente identificable de ellos o que el derecho interno imponga límites a dicho acceso por razones de salud u orden públicos o de seguridad nacional.

[15] Se han distinguido cuatro categorías de datos obtenidos en investigación: *raw data* (datos crudos de secuenciación), *general research findings*, *patient specific research findings*, y *patient-specific incidental findings*. La segunda categoría no es objeto de este derecho; claramente lo es la primera y la cuarta. En cuanto a la tercera, los autores opinan que también lo es aunque se trate de datos no validados científicamente. Kaye, Jane / Kanellopoulou, Nadja / Hawkins, Naomi / Gowans, Heather / Curren, Liam / Melham, Karen, "Can i access my personal genome? The current legal position in the UK", *Medical Law Review*, 0, 2013, doi:10.1093/medlaw/fwt027, pp. 23-25.

entendió que no era necesario, …). Esta cuestión es muy relevante teniendo en cuenta que es muy habitual la trasferencia de datos desde grandes repositorios de información para el desarrollo de proyectos concretos de investigación no concretados al inicio del tratamiento, también desarrollados por terceros.

4.2. La obligación de hacer efectivo el derecho

La obligación de satisfacer este derecho corresponde al responsable del fichero de los datos, que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" (art. 4.7 RGPD).

Cuando se traten los datos con fines de investigación, lo más frecuente será que el responsable sea el titular del fichero de la institución donde el profesional desempeñe su actividad. La identificación de esta figura es fundamental cuando se diseñan los procesos de tratamiento que implican circulación de datos, donde intervienen diferentes sujetos e instituciones. El titular de los datos debe saber a quién y cómo se tiene que dirigir para hacer efectivo su derecho.

Si los datos se almacenan en biobancos, el responsable del fichero es la persona física o jurídica que ostenta la titularidad del Biobanco y que se responsabiliza del mismo (art. 3 m del RD 1716/2011), y esto a pesar de que, según lo previsto en la LIB para la organización de los biobancos, estos establecimientos cuentan con un "responsable del fichero", que "atenderá las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación u oposición formuladas por los sujetos fuente, de conformidad con lo dispuesto en la normativa vigente sobre protección de datos de carácter personal" (art. 66.3). Esta figura, no recogida en la legislación sobre protección de datos, tendrá atribuidas estas funciones en la organización interna del funcionamiento de los biobancos, pero no asumirá las responsabilidades que atribuye la normativa al responsable del fichero.

Normalmente la información que se podrá facilitar desde los Biobancos que, como se sabe, son instituciones constituidas precisamente para facilitar el acceso a muestras biológicas humanas y datos asociados, será la relativa a las cesiones de datos y muestras para proyectos concretos, puesto que no almacenan los datos obtenidos en los proyectos a los que ceden las muestras. El derecho de acceso a estos otros datos se debe garantizar a través del acuerdo de transferencia de muestras; y deberá quedar atendido mediante

procedimientos adecuados, ya sea gestionando la solicitud del interesado presentada ante el Biobanco que puede actuar como intermediario entre sujeto e investigador, ya sea facilitando información sobre el modo en que ésta se deba sustanciar directamente ante quien es responsable de los datos obtenidos en los proyectos.

Este modelo, instituido en la LIB y en RD 1716/2011, es trasladable al caso en que se gestionen los datos en ficheros de otro tipo de instituciones, como hospitales o centros de investigación.

El derecho de acceso debería quedar garantizado también en relación con la información obtenida en proyectos desarrollados fuera del ámbito territorial de aplicación del RGPD a partir de datos trasferidos por un responsable situado en situado en España. Este responsable está sometido a las condiciones impuestas por el ordenamiento jurídico español para la obtención y tratamiento de los datos (lo cual abarca su cesión), que incluyen esta facultad.

4.3. Acceso a datos de fallecidos

El derecho personalísimo a la autodeterminación informativa se extingue con el fallecimiento. Los datos de personas fallecidas no son objeto del RGPD, cuyo considerando 27 recoge expresamente esta exclusión, si bien, a la vez, señala que los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de aquellas. El art. 2.2. b) de la LOPDyGDD reproduce este criterio, con una referencia a lo previsto en el artículo 3.

Siguiendo la tendencia de ampliar "el ámbito material de libertad de decisión del individuo sobre el destino para después de su muerte sobre una serie de asuntos de su esfera personal, a resultas de las consecuencias de la revolución tecnológica"[16], la Ley establece la obligación de respetar las disposiciones que indicara en vida el titular en relación con el tratamiento de los datos tras su fallecimiento, igual que puede hacer, por ejemplo, sobre el destino de sus órganos. El fallecido, en este caso, se quiso asegurar en vida de que sus datos iban a ser cancelados o que ciertas personas iban a acceder a determinada información.

[16] Minero Alejandre, Gemma, *La protección post mortem de los derechos al honor, intimidad y propia imagen y la tutela frente al uso de datos de carácter personal tras el fallecimiento*, Thomson Reuters Aranzadi, 2018, p. 31.

Así, el art.3.2. establece que "Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos".

Además, salvo objeción manifestada en vida por el fallecido, "Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante" (art. 3.1)[17].

A sensu contrario, se debe entender que los datos de fallecidos no pueden hacerse públicos, ni pueden cederse sin tener en cuenta lo que se acaba de señalar, no tanto porque sigan siendo objeto de protección de la LOPDyGDD (no se aplicarían por consiguiente el régimen sancionador previsto en esta norma), sino en tanto puedan afectar la protección de la personalidad pretérita, que ampara nuestro ordenamiento jurídico (LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen). El tratamiento de datos de personas fallecidas sólo constituirá infracción (leve) según la LOPDyGDD, cuando no se haya procedido a la supresión conforme el artículo 3 (art. 74 letra g).

En definitiva, esta posibilidad no deriva de una atribución de titularidad de los datos del fallecido a quienes están legitimados para ejercer el derecho de acceso, sino del interés en el cumplimiento de la voluntad que el fallecido expresó en vida o de la protección de la personalidad pretérita.

Cuando se accede por parte de terceros con otros propósitos, por ejemplo, la protección de su propia salud, o intereses patrimoniales, no se estará ejerciendo una facultad que integra el derecho a la autodeterminación informativa, sino otra que el ordenamiento jurídico pueda reconocer.

---

[17] Para un análisis de este artículo, véase Minero Alejandre, Gemma, *op. cit*, pp. 149 y ss.

En particular, la LAP prevé la posibilidad de acceso a historias clínicas de fallecidos (art. 18.4) y la LIB la de obtener muestras de cadáveres para su análisis o examinar las que estuvieran almacenadas en repositorios clínicos (art. 48.2 de la LIB)[18]. En la LAP están previstas dos posibilidades: primera, se permitirá el acceso a la historia a las personas vinculadas al fallecido siempre que no conste oposición de aquél; segunda, el acceso de terceros motivado por un riesgo para la salud (terceros vinculados o no al paciente). En este segundo supuesto el acceso se limita a ciertos datos, no a toda la historia, y se permitirá aun cuando el fallecido lo hubiera prohibido expresamente. En definitiva, la oposición del fallecido sólo es eficaz cuando no represente un riesgo para la salud. Continúa el artículo diciendo que no se facilitará información "que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros", advertencia que llama la atención porque la información de la historia clínica es en su gran mayoría "íntima", ya que se refiere a la salud del paciente, por lo tanto, cuando se permite el acceso (lo cual se está regulando en este apartado) se está facilitando información, si no fuera así las previsiones anteriores carecerían de sentido[19].

4.4. Limitaciones y excepciones

En relación con las posibles excepciones al derecho (véase lo que se dijo en el epígrafe 3.2), conviene recordar que la garantía de derecho de acceso tiene una importancia capital para asegurar el control del tratamiento de la información personal y que las excepciones deberían estar suficientemente justificadas, evaluadas por el CEI y aprobadas en el caso concreto. Esta regla general debería observarse todavía con más rigor cuando el sujeto no haya dado su consentimiento expreso y específico para el tratamiento de los datos, como puede ser el caso en supuestos de investigación biomédica.

---

[18] "Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite (…)". (art. 18.4 Ley 41/2002).
"En el ámbito sanitario se podrán obtener y analizar muestras de personas fallecidas siempre que pueda resultar de interés para la protección de la salud, salvo que el fallecido lo hubiese prohibido expresamente en vida y así se acredite. A tal fin serán consultados los documentos de instrucciones previas y, en su defecto, el criterio de los familiares más próximos del fallecido. El acceso de los familiares biológicos a la información derivada del análisis genético del fallecido se limitará a los datos genéticos pertinentes para la protección de la salud de aquéllos" (art. 48.2 LIB).

[19] Romeo, Carlos María / Nicolás, Pilar / De Miguel, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en la medicina personalizada de precisión*, Fundación Instituto Roche, Madrid, 2018, pp. 53 y ss.

Lo cierto es que las posibilidades de que el ejercicio del derecho de acceso a los datos por parte de un sujeto incidiera negativamente en la consecución de los objetivos de una investigación biosanitaria son remotas. Es difícil que pudieran verse afectados los derechos de los investigadores a la reserva de los resultados de su actividad (que sustentarán luego patentes o publicaciones), u otros intereses de la investigación (téngase en cuenta que el derecho no se refiere al acceso a procedimientos de análisis, ni a conclusiones, ni a resultados globales de la investigación). Cuestión distinta es que no sería descartable, más bien aconsejable, adoptar ciertas precauciones en la comunicación de la información requerida por el sujeto, como, por ejemplo, el acompañarla de la advertencia sobre su relevancia, trascendencia de su correcta interpretación, riesgos de su difusión, etc. No se trata en este caso de excepciones ni de limitaciones a su ejercicio.

5. El derecho a la supresión de los datos

El derecho a la supresión en el RGPD equivale al llamado anteriormente derecho a la cancelación, que ahora se regula en el contexto más amplio de los motores de búsqueda en internet (entorno en el que se denomina derecho al olvido)[20].

5.1. Principios relativos al tratamiento de datos y derecho a la supresión

Como es sabido el tratamiento de los datos debe cesar cuando deje de estar justificado por el fin que lo justificó. En este sentido, la supresión deriva del principio de calidad de los datos y es una manifestación de la congruencia con el título que legitimó el archivo para unos fines determinados. Pero, además, la supresión de los datos es una obligación del responsable si lo solicita el interesado, que decide, sin necesidad de justificación, el cese en el tratamiento.

Frente a este derecho, en el ámbito biomédico existen distintos deberes de mantenimiento de los datos, con distinto fundamento, desde cuestiones relativa a la responsabilidad profesional, hasta de seguridad de productos (por ejemplo, el deber de mantener los datos la historia clínica, de archivos de un ensayo clínico con medicamentos, o de registros de enfermedades,

[20] Álvarez Caro, María, "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", Piñar, José Luis (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Ed. Reus, Madrid, España, 2017, p. 233.

etc.). Normalmente las legislaciones establecen un periodo, durante el cual, el derecho de cancelación queda limitado en estos casos.

Igualmente, el derecho a la supresión puede incidir en derechos de terceros como, por ejemplo, de los investigadores que han invertido su esfuerzo en la generación y análisis de los datos y que pueden ver comprometidos los resultados de sus proyectos si los sujetos exigen su supresión. Por esta razón, en ocasiones se ha previsto también en estos supuestos una limitación a este derecho.

El RGPD Reglamento General de Protección de Datos recoge este derecho en su artículo 17 que establece que el responsable suprimirá los datos, a solicitud del interesado cuando concurra, entre otras, alguna de las siguientes circunstancias:

- Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

- El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico.

- El interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2.

- Los datos personales hayan sido tratados ilícitamente.

El reconocimiento de este derecho no implica que si no se ejerce el responsable, como regla general, pueda continuar tratando los datos si no subsiste el fin que justificó su recogida, en virtud de los principios que rigen la regulación del derecho a la autodeterminación informativa, en particular, los principios de minimización del tratamiento y limitación del plazo de conservación (art. 5, letras c y f RGPD)[21]. Ahora bien, incluso cuando el

[21] "1. Los datos personales serán: (…) c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); (…) e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio

tratamiento mantenga su legitimidad, el responsable debe suprimir los datos ante la solicitud del titular que decide sin necesidad de justificación el cese en el tratamiento. En esta vertiente, el derecho a la cancelación y el derecho a la revocación del consentimiento para el tratamiento están estrechamente relacionados. Si el título que legitimara el tratamiento fuera distinto al consentimiento, la relación se establecería, en su caso, con el derecho a la oposición al tratamiento (art. 21.6 RGPD)[22].

La LIB recoge con carácter general la facultad de revocación del consentimiento para investigación (art. 4.3) sin necesidad de aducir motivo alguno, y de forma específica en relación con el uso de muestras biológicas que, lógicamente, solo se podrá ejercer si la muestra no ha sido anonimizada. En este caso, el artículo 60.3 establece que "el consentimiento podrá ser revocado, totalmente o para determinados fines, en cualquier momento (…). Lo mismo ocurre en el caso de los ensayos clínicos (art. 4.3 del RD 1090/2015).

La cancelación de datos como vertiente o efecto del derecho a la revocación del consentimiento previsto por el ordenamiento jurídico se debería llevar a cabo de forma automática sin una solicitud añadida a la de dicha revocación. Han de articularse mecanismos que garanticen que la voluntad del titular llega al responsable del tratamiento de los datos, para que pueda tomar las medidas correspondientes cuando la revocación del consentimiento se ejerce ante persona distinta, por ejemplo, ante el investigador principal del proyecto, que trabaja en una institución y que maneja los datos como usuario autorizado, pero que no es el responsable del tratamiento.

Estos efectos deben estar descritos en la información previa al consentimiento inicial para asegurar que el sujeto conoce las consecuencias que tendrán sus decisiones en el futuro: "Antes de emitir el consentimiento para la utilización de una muestra biológica con fines de investigación biomédica que no vaya a ser sometida a un proceso de anonimización, el sujeto fuente recibirá la siguiente información por escrito: (…) e) Derecho de revocación del consentimiento y sus efectos, incluida la posibilidad de la destrucción o de la anonimización de la muestra y de que tales efectos no se extenderán a

de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ('limitación del plazo de conservación')".

[22] "6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público".

los datos resultantes de las investigaciones que ya se hayan llevado a cabo" (art. 59 de la LIB).

Del mismo modo, el nuevo RGPD dispone que "el interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo" (art. 73).

5.2. Supresión de datos de fallecidos

Como se dijo en el apartado 5.2, el derecho personalísimo a la autodeterminación informativa se extingue con el fallecimiento, pero el artículo 3 de la LOPDyGDD recoge mecanismos para proteger la personalidad pretérita y para que se cumpla la voluntad del fallecido expresada en vida.

En particular, por lo que se refiere a la supresión de datos en el marco de la investigación, el Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica señala: "Las personas vinculadas a la persona fallecida por razones familiares o análogas podrán dirigirse a los responsables de los ficheros o de los tratamientos que contengan datos de dicha persona fallecida con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, justificando la concurrencia de un interés relevante, la cancelación de los datos o la anonimización de las muestras" (art. 26.2).

Se debe advertir que la supresión en estos casos debe responder a la protección de un interés relevante acreditado, partiendo de que el tratamiento de los datos con fines de investigación biomédica no pierde la base legítima que lo justificó por el hecho del fallecimiento del titular.

5.3. Excepciones y limitaciones

La LOPDyGDD no menciona el derecho a la supresión entre aquellos cuyo ejercicio puede admitir excepciones, tampoco la correspondiente disposición del artículo 89 del RGPD. Esto no significa que esta posibilidad no exista, puesto que la recoge el artículo 17 RGPD, como se verá, pero

su interpretación debería tener en cuenta aquella omisión, así como otras previsiones de nuestro ordenamiento jurídico en relación con su ejercicio cuando se almacena información con fines de investigación[23].

En efecto, en nuestro ordenamiento jurídico, el derecho a la supresión en este contexto está estrechamente vinculado al de revocación del consentimiento para participar en la investigación. Este derecho tiene un evidente y rotundo efecto prospectivo, pero más limitado en relación con la actividad que los investigadores realizaron en el pasado al amparo de un consentimiento que la legitimaba. Es decir, no se considera del mismo modo la supresión de datos almacenados en un estudio que ya se realizó y la de datos almacenados para su posterior utilización en investigación.

Por eso, La LIB advierte que "(…) Cuando la revocación se refiera a cualquier uso de la muestra, se procederá a su inmediata destrucción, sin perjuicio de la conservación de los datos resultantes de las investigaciones que se hubiesen realizado con carácter previo" (artículo 60.3). En esta línea, el RD 1090/2015 señala que: "(…) La retirada del consentimiento no afectará a las actividades realizadas en base a su consentimiento antes de haberlo retirado, garantizando a su vez que ni los datos ni las muestras obtenidas en base a dicho consentimiento podrán emplearse en análisis ni estudios posteriores a la fecha de retirada (…)".

Se protege así el interés de los investigadores en relación con los resultados de su actividad profesional y los derechos sobre misma, a la vez que la necesidad de mantener los datos a efectos de trazabilidad de la actividad o posibles reclamaciones[24]. Por consiguiente, la revocación del consentimiento

---

[23] Advierte sobre esta aplicación directa del artículo 17 Manis, Maria Luisa, "The processing of personal data in the context of scientific research. The new regime under the EU-GDPR ", *Biolaw Journal/Rivista di Biodiritto,* Núm. 3, 2017, p. 340.

[24] Por eso, el RD 1090/2015, por el que se regula los ensayos clínicos con medicamentos establece la obligación de mantener documentación relativa al ensayo, tanto para los Comités de Ética durante un mínimo de tres años (art. 16.7), como para el promotor y el investigador durante un mínimo de veinticinco años (art. 43).
En cuanto a la documentación de la historia clínica, la Ley 41/2002 señala que se conservará "durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial" (artículo 17.1). Además "La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas" (art. 17.2). Finalmente, la LIB también contiene algunas previsiones relativas a la obligación de mantenimiento de los datos durante treinta años para casos concretos en que sea

no supondrá la supresión o eliminación de los datos, que deben conservarse para atender eventuales responsabilidades derivadas del tratamiento, o para sustentar los resultados de la investigación. Pero dado que estas exigencias no pueden suponer una vulneración del derecho de los sujetos a su intimidad y control de su información, si el consentimiento se revoca los datos quedarán "bloqueados" (solo se utilizarán para atender aquellas responsabilidades) y únicamente podrán publicarse o cederse de manera agregada sin que sea posible la identificación de los sujetos. La obligación de confidencialidad de quienes están involucrados en la investigación subsiste como garantía de la privacidad de los sujetos. Además, debería considerarse si la anonimización de los datos (sin proceder a su supresión) sería una medida adecuada para conciliar todos los intereses en juego.

Por el contrario, el efecto de la revocación del consentimiento sobre el uso prospectivo de los datos debe ser su supresión, sin que se prevean matices al respecto. Es cierto que el RGPD prevé una posible excepción genérica, en el apartado 3 del artículo 17 cuando advierte que la obligación de supresión no se aplicará cuando el tratamiento sea necesario (…) d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento (…)". Si bien esta previsión podría suponer un paso más allá de las limitaciones derivadas de las condiciones antes descritas (protección de los resultados del trabajo y obligación de archivo de documentación), no parece que pueda justificarse fácilmente para continuar obteniendo o utilizando datos en investigación tras la revocación del consentimiento, teniendo en cuenta los efectos que específicamente la LIB otorga a este acto[25]. El mantenimiento de datos

---

preciso asegurar la trazabilidad de células y tejidos que se hayan aplicado en humanos con fines de investigación (art. 8), igual que en la legislación sobre trasplante (art. 22 del RD 1723/2012, de 28 de diciembre, por el que se regulan las actividades de obtención, utilización clínica y coordinación territorial de los órganos humanos destinados al trasplante y se establecen requisitos de calidad y seguridad; y 33 del RD-ley 9/2014, de 4 de julio, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos y se aprueban las normas de coordinación y funcionamiento para su uso en humanos).

Véase también la Recomendación de la Comisión de la Unión Europea de 25.4.2018 on access to and preservation of scientific information.

[25] Como se ha dicho, "Naturally, it is quite difficult if not impossible to retroactively remove a person's data from research conclusions. However, in terms of prospective research this should not be the case (i.e. it should be possible for the data subject to ask for their data to be removed from any databases to avoid future processing for research

para investigaciones futuras frente a una solicitud de supresión, es decir, con oposición del sujeto , debe estar limitada a supuestos de extraordinaria necesidad (Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública).

6. Derecho a la rectificación

De acuerdo con el principio de exactitud, los datos deber ser "exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan" (art. 5 letra de RGPD).

En virtud de este principio, el interesado tiene derecho a que se rectifique o se complete la información objeto de tratamiento para que los datos sean veraces (art. 16 RGPD).

No parece que el derecho a que se rectifiquen o se completen los datos inexactos tenga una gran trascendencia en la investigación biomédica (puede tener más relevancia, por ejemplo, en la investigación histórica). Tampoco su limitación. La metodología de la investigación científica requiere la exactitud y fiabilidad de la información que se maneja para obtener conclusiones sólidas, de manera que será en su propio interés la exigencia de dicha exactitud; por otra parte, en cuanto a otros datos o conclusiones que se obtienen, precisamente como fruto de la investigación, podrán tener un significado incierto (es el terreno de investigación y no de la mayor certeza exigible en la práctica clínica). La inexactitud de los datos en la investigación científica no afecta tanto a los derechos individuales de los sujetos como al rigor de la actividad y, por consiguiente, a los propios investigadores.

7. El derecho a ser informado de los datos relevantes para la salud

7.1. La base jurídica del derecho

Los artículos 4.5 y 26 de la LIB señalan que si en la investigación se encontrara información relevante para la salud de los participantes, deberá

purposes)", Pormeister, Kärt, "Genetic data and the research exemption: is the GDPR going too far?", *International Data Privacy Law*, Núm. 2, Vol. 7, 2017, p. 141.

ser puesta a su disposición "en el marco de la asistencia en curso o, en su defecto, prestando un asesoramiento específico".

Se reconoce así un derecho cercano al derecho de acceso a los datos personales, pero de naturaleza distinta, no derivado del poder de control sobre la información personal, y que otorga al sujeto la facultad de tomar una posición en relación con la comunicación de la información que sea relevante para su salud (art. 4.5 segundo párrafo y 59.1.i. de la LIB).

El reconocimiento de este derecho, que también figura en la Declaración Internacional sobre los datos genéticos humanos de la Unesco[26], es un claro ejemplo de la permeabilidad de las fronteras que separan investigación y asistencia clínica. En efecto, el posible beneficio directo para la salud que se pudiera derivar de los resultados de la investigación, hace nacer una obligación para los investigadores que desarrollan una actividad en un contexto diferente al asistencial, con otras reglas y requisitos. El objetivo de la investigación científica es buscar un conocimiento generalizable, no un beneficio individual para el sujeto que aporta muestras o datos, al contrario de lo que ocurre con la actividad asistencial, cuyo principal objetivo es procurar un beneficio a un paciente.

Es preciso recordar que no obstante la existencia de esta obligación de comunicar, si es que así lo decidió el sujeto, la relación entre investigador y sujeto se mantiene en un contexto de investigación, sin que se establezca un vínculo distinto ni una relación médico-paciente. Por esta razón, no existe un deber para el investigador de buscar información con un propósito diagnóstico, fuera de lo que su proyecto requiera[27].

---

[26] Artículo 10. Derecho a decidir ser o no informado de los resultados de la investigación: "Cuando se recolecten datos genéticos humanos, datos proteómicos humanos o muestras biológicas con fines de investigación médica y científica, en la información suministrada en el momento del consentimiento debería indicarse que la persona en cuestión tiene derecho a decidir ser o no informada de los resultados de la investigación. En su caso, los familiares identificados que pudieran verse afectados por los resultados deberían gozar también del derecho a no ser informados".

[27] Sin embargo, Gliwa y Berkman, opinan que la disponibilidad de medios con que cuentan los investigadores no justifica, por sí sola, la obligación de que lleven a cabo análisis con finalidad diagnóstica pero sí cuando concurren otras circunstancias (utilidad de la información, que no es accesible por otras vías, y esfuerzo razonable para obtenerla). Los autores concluyen que, en principio, esa obligación no existe pero que podrá surgir en el proceso de traslación de los resultados de la investigación al contexto clínico. Gliwa, Catherine / Berkman, Benjamin E., "Do Researchers Have an Obligation to Actively Look for Genetic Incidental Findings?", *American Journal of Bioethics*, Núm. 2, Vol. 13, 2013, pp. 7 y 15.

Por el contrario, la opción por la ignorancia debe ser respetada como manifestación del derecho a no saber, que tiene un peso mayor en el ámbito de la investigación que cuando se ejerce en el marco de un tratamiento médico, caso en el que queda limitado por las necesidades del tratamiento libremente aceptado (LAP)[28], lo que no ocurre si el análisis no se lleva a cabo en un contexto asistencial.

Si el sujeto ha optado por la ignorancia, según el artículo 49 de la LIB "se podrá" informar a los afectados (que no titulares de los datos) o a su representante legalmente autorizado. El artículo 5.5 de la misma ley prevé a estos efectos un procedimiento que encaja más bien con la gestión de descubrimientos en el marco de análisis clínicos puesto que menciona al "médico responsable", si bien en cualquier caso sí parece adecuada la intervención del Comité Asistencial del centro si lo hubiera (a lo que también se refiere este artículo). Por otra parte llama la atención que mientras el artículo 49 utiliza la expresión "se podrá informar", el 5.5 de la misma ley señala que "se informará". De nuevo parece que este artículo se enfoca hacia una situación de proceso de consejo genético clínico en el que los familiares están ya implicados en el análisis.

7.2. Mecanismos de garantía

La garantía de este derecho requiere el diseño de procedimientos que involucren a los sujetos e instituciones involucrados en el circuito de los datos, tanto de carácter clínico como de investigación básica. El derecho se desenvuelve en las siguientes fases cuando interviene un Biobanco, supuesto previsto con más detalle en la legislación y aplicable a otros casos:

Más contundente en otra posición son Dal-Ré, Rafael / Katsanis, Nicholas / Katsanis, Sara / Parker, Lisa S. / Ayuso, Carmen, en "Managing Incidental Genomic Findings in Clinical Trials: Fulfillment of the Principle of Justice", *PLoS Med*, Núm. 1, Vol. 11, 2014, p. 2. Los autores sostienen que "it seems appropriate to apply a standard-of-care list of genes for which to actively seek pathogenic variants in clinical research. If, as standard of care, a patient could be informed of particular variants reported as actionable incidental genomic findings when visiting a physician, it is reasonable to argue that the same patient, as a participant in a trial involving WGS/WES, may have the right to be informed about those same incidental genomic findings".

[28] Artículo 9. Límites del consentimiento informado y consentimiento por representación: "1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención".

Primero, el sujeto debe ser informado sobre la posibilidad de que, si sus muestras o datos se utilizan con fines de investigación, es posible que se obtenga nueva información que pueda ser relevante para su salud o a la de sus familiares. El sujeto deberá manifestar su voluntad en relación con la futura comunicación de esta nueva información (art. 59.1.i LIB).

A diferencia de lo que supone el derecho de acceso, el derecho a ser informado de los datos relevantes para la salud genera una obligación de informar sin que se precise una solicitud expresa si es que el sujeto hubiera optado por la comunicación con carácter previo, en el momento en que decidió participar en la investigación. En ese momento se le debió plantear la posibilidad de elegir entre una u otra opción. Cuando esa decisión no conste (si, por ejemplo, los datos fueron utilizados sin consentimiento expreso para investigación cuando un CEI lo aprobó), posteriormente será preciso llevar a cabo un ejercicio de presunciones que incluirá también como factor a tener en cuenta, el posible deseo de no conocer cierto tipo de información.

Segundo, si el investigador descubre información que a su juicio pueda ser relevante para la salud del sujeto deberá comunicarlo al Comité de Ética Externo del Biobanco y/o al Comité de Ética evaluador del proyecto.

Tercero, se evaluará la relevancia para la salud de esta información. La normativa aplicable no detalla cómo o quién debe llevar a cabo esta valoración en particular, si bien está previsto que, en general, el Comité de Ética que evaluó el proyecto o el Comité de Ética Externo del biobanco decidan en qué casos será necesario que se envíe información de manera individualizada a los sujetos (RD artículo 23.2 del RD 1716/2011).

En cuanto al objeto de la obligación de comunicación abarca aquellos datos relevantes para la salud en un sentido amplio, también para la salud reproductiva, teniendo en cuenta la posibilidad de acudir a diagnósticos preconceptivos o preimplatacionales a partir del conocimiento de los datos. Será el investigador quien evaluará en primer lugar la relevancia y la validez de los resultados, como primer profesional que los conoce.

Para comunicar un resultado, éste debe cumplir los requisitos de presentar validez analítica y relevancia clínica[29]. La importancia clínica de la información dependerá de la penetrancia de la variante (probabilidad de que la característica controlada por un gen se manifieste en la persona portadora),

[29] Ayuso, Carmen / Millán, José María / Dal-Ré, Rafael, "Management and return of incidental genomic findings in clinical trials", *Pharmacogenomics*, 15(1), 2015, pp. 1 y ss.

la gravedad de la enfermedad que produce y de la posibilidad de intervención. No obstante, la oportunidad de comunicar la información también puede depender de otros factores, como su incidencia en la toma de decisiones reproductivas o de otro tipo. No se debe descartar, por consiguiente, la información sobre hallazgos relativos a enfermedades graves frente paraa las que no hay intervención posible, siempre que se tenga certeza de la validez de los resultados[30].

Cuarto, la información será trasladada al sujeto que, probablemente, pasará a ser "paciente" y, por lo tanto, se deberá situar en un contexto clínico. Esto significa que lo más adecuado sería que fuera un profesional clínico el que abordase esta etapa. En este sentido, el investigador debe garantizar la disponibilidad de consejo genético para el supuesto en que se vaya a comunicar esta información. Así lo prevé el art. 47.6º LIB (análisis genéticos clínicos) que será aplicable puesto que, dado el caso, como se advirtió más arriba, las fronteras entre área de investigación y área clínico se difuminan y las obligaciones propias de cada una de ellas se comunican. Esto no significa que el consejo genético se vaya a dispensar por ese mismo investigador, sino que se garantiza que el servicio será accesible.

7.3. Limitaciones y excepciones

Un acuerdo entre las partes (investigador y sujeto de la investigación) no podría ser contrario a esta obligación nacida de la Ley, en cualquier sentido que la contravenga. Sería nula una condición que estableciera, pongamos por caso, que el sujeto no va a ser informado de los datos relevantes para su salud que se obtuvieran en la investigación, u otra en la que se accediera a ser informado sin posibilidad de optar por la ignorancia. El sujeto siempre debe tener la oportunidad de decidir.

Ahora bien, no se encuentran argumentos jurídicos que impidan la posibilidad de excluir del proyecto de investigación a los sujetos en función de su decisión, teniendo en cuenta que no existe un derecho a la participación en la investigación biomédica. En este supuesto, el Comité de Ética correspondiente que revisa los proyectos, y que examina los criterios de selección de los sujetos, debería valorar en el caso concreto si la exclusión es admisible según los principios que aplica en sus evaluaciones y que van más allá de los razonamientos jurídicos. Por ejemplo, se podría dar el caso

[30] Ayuso, Carmen / Millán, José María / Dal-Ré, Rafael, *Cómo manejar los hallazgos inesperados en investigación genética ¿Cuándo hay que comunicarlos? Luces y sombras en la investigación clínica* (Capítulo 10), Fundació Víctor Grífols I Lucas, 2013.

en que un investigador planteara excluir a quienes donaron muestras con fines de investigación en general y hubieran pedido no ser informados de los resultados de las investigaciones a las que se destinara su muestra en el futuro, porque supiera que en el proyecto se van a obtener datos sobre una enfermedad grave para la que existieran medidas preventivas eficaces; o, por el contrario, que quisiera excluir a los donantes que optaron por conocer los resultados y elegir a los que eligieron ignorarlos, para evitar las gestiones que le supondrían el retorno de resultados.

8. El derecho a conocer los resultados globales de la investigación

El derecho a conocer la información relativa a los resultados de una investigación se fundamenta en una concepción del sujeto como verdadero partícipe en esta actividad, y no como una mera fuente de datos, experimentos o muestras: el individuo pasa a estar involucrado en el desarrollo de los proyectos y, por lo tanto, ostenta un interés legítimo en conocer su evolución y conclusiones. Si bien el cuerpo, las células, tejidos o datos son *objeto* de la investigación, el individuo es un *sujeto* que participa en esta actividad.

En este sentido, el artículo 27 de la LIB establece lo siguiente:

> "1. Una vez concluida la investigación, el investigador responsable remitirá un resumen de la misma a la autoridad competente que dio la autorización y al Comité de Ética de la Investigación correspondiente. 2. Los resultados de la investigación se comunicarán a los participantes, siempre que lo soliciten. (…)".

El titular de este derecho es el "sujeto participante en la investigación", término que se refiere al que se somete con este fin a una intervención invasiva o dona sus muestras ("sujeto fuente") o facilita sus datos (titular de los datos).

Ahora bien, el consentimiento del sujeto no implica su participación efectiva, sino potencial. Sólo cuando la intervención invasiva se ha producido o el material para la obtención de datos está disponible, se puede afirmar que un individuo pasa a estar involucrado y formar parte del proyecto, eso sí, también cuando la intervención no produzca resultados útiles, las muestras se desechen o los datos no resulten de interés. El hecho es que el individuo ha iniciado en estos casos una participación efectiva, ha sido, como mínimo "evaluado" en el marco de una hipótesis científica específica, y por lo tanto, ha nacido ya aquel interés legítimo al que se aludió. De estas valoraciones se

deben excluir las que se llevan a cabo para hacer una selección de individuos con carácter previo al inicio de la investigación. Sería el caso, por ejemplo, de la selección de muestras que hace un biobanco para enviar a un investigador aquéllas que presentan las características que éste ha solicitado. En esta línea, pero a la inversa, la participación no depende de que se haya otorgado o no un consentimiento. Así, el individuo es *sujeto participante* en la investigación, aunque, por ejemplo, la intervención se hubiera llevado a cabo estando inconsciente, o las muestras se hubieran utilizado sin informar previamente a quien se consideraba ilocalizable, o los datos se refirieran a quien no tenía madurez para comprender la naturaleza de la cesión.

El contenido del derecho a ser informado de los resultados de la investigación se refiere a la facultad de exigir que se responda a una solicitud del sujeto. La obligación de informar no existe hasta que se presenta esa solicitud, aunque sería una buena práctica articular mecanismos de difusión de los resultados de manera que pudieran llegar al mayor número de participantes, sin esperar a que se dirigieran al investigador o al biobanco.

La información sobre la vía para ejercer el derecho es imprescindible y debe ser previa al consentimiento. La LIB recoge esta obligación en su artículo 15: "1. Las personas a las que se solicite su participación en un proyecto de investigación recibirán previamente la necesaria información, debidamente documentada y en forma comprensible y cuando se trate de personas con discapacidad de forma adecuada a sus circunstancias. 2. (…) Dicha información especificará los siguientes extremos: (…) e) Medidas para acceder, en los términos previstos en el artículo 4.5, a la información relevante para el sujeto, que surja de la investigación *o de los resultados totales*".

En términos parecidos, pero más acertados, el artículo 13 del Protocolo Adicional al Convenio de Biomedicina del Consejo de Europa sobre Investigación Biomédica, de 2005, incluye, entre la información que se debe transmitir cuando se solicita el consentimiento para participar en una investigación, la relativa a los "*arrangements for access to information relevant to the participant arising from the research and to its overall results*". En esta redacción queda más claro que el sujeto tiene derecho a conocer resultados relevantes para él mismo, y también resultados generales. Por eso, el artículo 15 de la LIB debería recoger la referencia al 4.5 inmediatamente antes del término "o de los resultados totales", y emplear la conjunción "y", en lugar de "o": "Medidas para acceder a la información relevante para el sujeto que surja de la investigación, en los términos previstos en el artículo 4.5, y a los resultados totales".

Lógicamente, si la vía para acceder a los datos relevantes para la salud y la prevista para acceder a los resultados totales es la misma, no es preciso que se repita: lo relevante es que el sujeto conozca sus derechos y sepa que existe una vía de comunicación para ejercerlos.

Ni la LIB ni el Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica, ni tampoco el Protocolo sobre Investigación Biomédica citado, describen cómo se debe responder a la solicitud. No parece imprescindible que se haga de una manera personalizada, siempre que se garantice la efectividad. Por ejemplo, la disponibilidad de esta información en una página web (referenciada en la información previa al consentimiento o tras una solicitud) podría ser suficiente, salvo que se planteara algún inconveniente particular.

Por otra parte, para determinar quiénes quedan obligados a satisfacer este derecho, ayuda recordar que el artículo 32 del Real Decreto 1716/2011, dispone: "(…) el biobanco, el responsable de la colección y el responsable del proyecto en el que se utilicen muestras biológicas de origen humano con fines de investigación biomédica facilitarán al sujeto fuente la disponibilidad de la información relativa a la utilización de su muestra por parte de terceros, salvo que aquélla hubiera sido anonimizada, y en concreto: (…) b) Beneficios esperados y alcanzados".

Según este artículo, el biobanco, al responsable de la colección y al responsable del proyecto en que se utilicen las muestras, serán quienes "facilitarán al sujeto fuente la disponibilidad de la información relativa a la utilización de su muestra por parte de terceros, salvo que aquélla hubiera sido anonimizada. Esta responsabilidad no es subsidiaria sino solidaria (la redacción no establece una enumeración alternativa de los obligados): los investigadores que utilicen muestras procedentes de un biobanco deberán a su vez garantizar que, del modo que quede establecido, trasladarán la información para que pueda llegar al participante por vía del Biobanco[31].

[31] Recuérdese que en nuestro ordenamiento existen tres regímenes de utilización de muestras con fines de investigación científica. Si se han donado para un proyecto, la relación del sujeto se establece directamente con el investigador principal, si a una colección, con el responsable de la misma, que estará involucrado en las futuras investigaciones que se realicen con la muestra. En estos dos supuestos IP y responsable de la colección conocen los resultados y los pueden facilitar a quien los soliciten. Sin embargo, es posible que se donen

Aunque el Real Decreto no prevé expresamente obligaciones para los centros donde los investigadores desarrollen su trabajo, existirá responsabilidad institucional cuando se vulneren los derechos de los sujetos en el curso de una actividad que se desarrolla bajo su jurisdicción.

En cuanto al objeto del derecho, recordemos que en las disposiciones citadas se menciona "resultados totales" (LIB), "overall results" (Protocolo sobre Investigación Biomédica del Consejo de Europa), o "beneficios alcanzados" (RD 1716/2011). Pues bien, aunque el último término alude a un objeto más reducido (y algo ambiguo) puesto que se limita a los resultados *beneficiosos*, no hay razón para que se omitan, tal como recoge el artículo 27 de la LIB, todos los resultados de la investigación, sin descartar los que no hayan reportado avances o beneficios.

Finalmente, queda plantear durante cuánto tiempo se puede ejercer este derecho y hasta cuándo subsiste la consiguiente obligación por parte de investigadores, responsables de colecciones y biobancos de satisfacer la solicitud. En principio, no existe un plazo o una condición que determine su extinción, ni se ha señalado un periodo determinado para la obligación de mantener la información disponible que recoge el RD 1716/2011. En el caso de biobancos, teniendo en cuenta las previsiones de sostenibilidad de estas instituciones y el largo periodo de tiempo durante el que almacenan y se dispone de las muestras, podría sostenerse la obligación de conservar esta información mientras dure su actividad y, más allá, según los casos, se debería trasladar en las condiciones previstas en caso de cierre[32]. Más complejo es el supuesto en que los resultados se archiven en el contexto de colecciones o proyectos concretos, casos en que no existe de forma tan evidente en la práctica un respaldo institucional con mecanismos y procedimientos que permitan satisfacer las solicitudes de información sobre los resultados de las investigaciones más allá de las posibilidades con que cuentan los investigadores. Por eso, lo más adecuado sería que los centros donde se constituyen las colecciones o se desarrollan los proyectos implantaran unas políticas en conexión con sus Comités de Ética y asumieran responsabilidades en esta

muestras a biobancos para que estas instituciones, a su vez, las cedan a investigadores. En este caso, el biobanco, actúa como un mediador entre el investigador y el donante.

[32] Artículo 11 del RD 1716/2011. Cierre del biobanco a solicitud de su titular: "1. La persona titular de un biobanco podrá solicitar su cierre a las autoridades competentes para autorizar su constitución y funcionamiento. 2. En la resolución de cierre se dispondrá expresamente el destino de las muestras almacenadas en el biobanco, oída la persona titular del mismo. Dicho destino podrá consistir en: a) La destrucción de las muestras. b) La cesión de las muestras a otro biobanco. c) La conservación de las muestras para su utilización en proyectos de investigación concretos o integradas en una colección".

materia. Conviene recordar que estos centros son responsables también de la protección de los derechos de los sujetos en el curso de una actividad que se desarrolla bajo su jurisdicción.

Para concluir, conviene recordar que, si bien el derecho a conocer los resultados globales de la investigación no ha merecido mucha atención en la práctica ni se suele mencionar en la información previa al consentimiento para la participación en la investigación, puede desempeñar un papel muy relevante para fomentar la participación, y es una manifestación del respeto a los sujetos cuya colaboración es imprescindible para desarrollar esta actividad[33].

9. Conclusión

El RGPD representa un cambio para la regulación del tratamiento de datos en la investigación biomédica en relación con la anterior normativa comunitaria. El texto reconoce el interés social del progreso de la ciencia y refleja explícitamente la intención de evitar obstáculos para su desarrollo, que hoy se desenvuelve en gran medida a través de nuevas herramientas tecnológicas. Con este propósito el Reglamento articula mecanismos que concilian la promoción de estos avances con la protección del derecho a la autodeterminación informativa de los sujetos. Además, los procedimientos de control de la actividad biomédica, ya implantados o propuestos, se acomodan bien al nuevo modelo de protección de datos en el que se incrementa la idea de responsabilidad proactiva y la autorregulación.

Este nuevo enfoque se refuerza y se hace más exigente en el ámbito de la investigación científica, en el que se exige para el tratamiento de datos, en todo caso, "garantías adecuadas" a través de la implantación de particulares "medidas técnicas y organizativas". Esta condición es la piedra angular de un sistema que, a partir de aquí, abre la puerta a la posible flexibilización del régimen general en algunos aspectos.

El desarrollo de esta oportunidad a través de la LOPDyGDD debe ser bienvenida, puesto que colma una laguna en nuestro ordenamiento. Sin embargo, quizás hubiera sido más acertado su incorporación en la LIB, como

[33] Macneil, S.D. / Fernández, C.V., "Informing research participants of research results: analysis of Canadian university based research ethics board policies", *Journal of Medical Ethics,* Núm. 1, Vol. 32, 2006, p. 50. Kerasidou, Angeliki, "Sharing the knowledge: sharing aggregate genomic findings with research participants in developing countries", *Developing World Bioethics*, Núm. 3, Vol. 15, 2015, p. 274.

norma relativa precisamente al contexto de la investigación biomédica y que regula procedimientos muy cercanos, incluso confluyentes al regulado ahora en la DA17ª de la LOPDyGDD. Probablemente esta aproximación sistemática hubiera llevado aparejada una revisión más detenida de las disposiciones de la LIB y un encaje más armonioso de distintas normas relativas a procedimientos muy próximos en la metodología de la investigación biomédica.

Se reconocen de manera equivalente, otras bases jurídicas, distintas al consentimiento para tratar los datos de carácter personal relativos a la salud y los datos genéticos, en particular cuando se trata de finalidad científica. Es importante subrayar que estas otras bases jurídicas no podrán sustentar el tratamiento si suponen que las garantías para los derechos de los titulares quedan debilitadas. Esta condición exige que los derechos del titular sobre sus datos estén nítidamente definidos y protegidos, lo que puede incluso significar un mecanismo que otorgue un control incluso más reforzado que la firma del consentimiento.

Estos derechos comparten algunos elementos, pero tienen una naturaleza diferente. Tampoco su desarrollo normativo y su implementación han sido equivalentes, y por eso en algunos casos son precisos más esfuerzos para hacerlos efectivos, tanto por parte de investigadores como de sus instituciones y comités de ética. El consenso para determinar los criterios que se deben seguir en esta línea, así como su aplicación homogénea, favorecería la seguridad de todos los implicados.

En este sentido, partiendo de que la institucionalización y obligatoriedad del control del tratamiento de datos en investigación biomédica por parte de los Comités de Ética de la Investigación, es también un paso positivo, es aconsejable que, en el desarrollo normativo de estos procesos, actualmente en un estado muy inicial, se tengan en cuenta estas nuevas atribuciones y los retos que plantean y se implanten procedimientos ágiles, eficaces, y garantistas para hacer efectiva esta atribución.

10. Bibliografía

Agencia Española de Protección de Datos, Código de buenas prácticas en protección de datos para proyectos big data, 2018.

Álvarez Caro, María, "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", Piñar, José Luis (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Ed. Reus, Madrid, España, 2017.

Ayuso Carmen / Millán José María, Dal-Ré / Rafael, "Management and return of incidental genomic findings in clinical trials", *Pharmacogenomics*, Núm. 1, Vol. 15, 2015.

Ayuso Carmen / Millán José María, Dal-Ré / Rafael, *Cómo manejar los hallazgos inesperados en investigación genética ¿Cuándo hay que comunicarlos? Luces y sombras en la investigación clínica* (Capítulo 10). Fundació Víctor Grífols I Lucas, 2013.

Dal-Ré, Rafael / Katsanis, Nicholas / Katsanis, Sara / Parker, Lisa S. / Ayuso, Carmen, "Managing Incidental Genomic Findings in Clinical Trials: Fulfillment of the Principle of Justice", *PLoS Med*, Núm. 1, Vol. 11, 2014.

Donnelly, Mary / Mcdonagh, Maeve,"Health Research, Consent and the GDPR Exemption", *European Journal of Health Law*, Núm. 2, Vol. 26, 2019.

Dove, Edward, "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era", *The Journal of Law, Medicine & Ethics*, Núm. 4, Vol. 46, 2018.

Gil, Elena, *Bigdata, Privacidad y protección de datos*, Agencia Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, España, 2016.

Gliwa, Catherine / Berkman, Benjamin E., "Do Researchers Have an Obligation to Actively Look for Genetic Incidental Findings?", *American Journal of Bioethics*, Núm. 2, Vol. 13, 2013.

Hernández Corchete, Juan Antonio, "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", José Luis Piñar (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Ed. Reus, Madrid, España, 2017.

Kaye, Jane / Kanellopoulou, Nadja / Hawkins, Naomi / Gowans, Heather / Curren, Liam / Melham, Karen, "Can i access my personal genome? The current legal position in the UK", *Medical Law Review*, 0, 2013.

Kerasidou, Angeliki, "Sharing the knowledge: sharing aggregate genomic findings with research participants in developing countries, *Developing World Bioethics*, Núm. 3, Vol. 15, 2015.

Lapunzina, Pablo / Nicolás, Pilar (Coords.), *Gestión de datos genómicos con finalidad clínica y de investigación*, Idemm Farma, Madrid, España, 2015.

Macneil, S.D. / Fernández, C.V., "Informing research participants of research results: analysis of Canadian university based research ethics board policies", *Journal of Medical Ethics,* Núm. 1, Vol. 32, 2006.

Manis, Maria Luisa, "The processing of personal data in the context of scientific research. The new regime under the EU-GDPR ", *Biolaw Journal/Rivista di Biodiritto*, Núm. 3, 2017.

Minero Alejandre, Gemma, *La protección post mortem de los derechos al honor, intimidad y propia imagen y la tutela frente al uso de datos de carácter personal tras el fallecimiento*, Thomson Reuters Aranzadi, Cizur Menor, España, 2018.

Nicolas, Pilar, "Reglamento (UE) 2016/679 General de Protección de Datos: un nuevo marco normativo para el tratamiento de datos personales con fines de investigación biomédica", *Comentarios al Reglamento General de Protección*

de Datos y a Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, Antonio Troncoso Reigada (Dir), Thomsom Reuters Aranzadi, Cizur Menor, España, 2019.

Pormeister, Kärt, "Genetic data and the research exemption: is the GDPR going too far?", *International Data Privacy Law*, Núm. 2, Vol. 7, 2017.

Romeo, Carlos / Nicolás, Pilar / De Miguel, Iñigo, *Retos éticos y necesidades normativas en la actividad asistencial en la medicina personalizada de precisión*, Fundación Instituto Roche, Madrid, España, 2018.

Shabani, Mahsa / Borry, Pascal,, Pascal, "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation", *European Journal of Human Genetics*, Núm. 26, 2018.

Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, Barcelona, Noviembre de 2017.

Troncoso Reigada, Antonio, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano / Law and the Human Genome Review*, Núm. 49, 2018.

Implicaciones jurídicas de la internalización de la tecnología del *Big Data* y Derecho Internacional Privado*

Legal implications of the internalization of big data technology and private international law

Prof. Dr. Alfonso Ortega Giménez

Profesor Contratado de Derecho Internacional Privado en la Universidad Miguel Hernández (Alicante, España)

DOI: 10.14679/1136

Sumario / Summary: 1. ¿Qué es el *Big Data*? 1.1. Concepto. 1.2. Características: las *V´s*. 1.3. Clasificación de datos. 2. Implicaciones legales del *Big Data* susceptibles de problemas de Derecho Internacional Privado. 2.1. Implicaciones para la protección de datos. 2.2. Implicaciones en la protección legal del algoritmo y la base de datos. 2.3. Implicaciones legales en las relaciones contractuales. 2.4. Implicaciones legales en las relaciones laborales. 3. Afectación de las cuestiones legales desde la perspectiva del Derecho Internacional Privado. 3.1. Protección de datos. 3.2. Protección del algoritmo y las bases de datos. 4. Reflexiones finales. 5. Bibliografía.

Resumen / Abstract: Este trabajo tiene como objetivo explicar el concepto de *Big Data* y las consecuencias legales que, a nivel internacional, ha traído consigo el uso de esta tecnología. Somos conscientes que debido al avance tecnológico han irrumpido en el tejido empresarial una serie de organizaciones cuya actividad principal es la prestación de servicios de *Big Data*. Este estudio está dividido en tres grandes partes: en la primera de ellas, abordaremos el concepto de *Big Data* y las características que hacen tan singular esta tecnología, para así, entender el motivo por el cual se ha convertido en la herramienta fundamental de las empresas internacionales que

* Artículo recibido el 14 de octubre de 2018 y aceptado para su publicación el 9 de junio de 2019.
Dirección de correspondencia: alfonso.ortega@umh.es

se dedican a la prestación de servicios se tratamiento de datos; la segunda parte está dedicada a las implicaciones legales del *Big Data* susceptibles de problemas de Derecho internacional privado (la protección de datos, la protección legal del algoritmo y la base de datos, las relaciones contractuales y las relaciones laborales en las que se utiliza la tecnología *Big Data*); y, finalmente, la tercera parte, teniendo en cuenta la posible problemática que pueda surgir y la responsabilidad contractual y extracontractual que pueda generar el uso de la tecnología *Big Data*, consideramos de gran importancia abordar los temas relativos a la competencia judicial internacional y la determinación de la ley aplicable.

This work aims to explain the concept of Big Data and the legal consequences that, at international level, has brought with it the use of this technology. We are aware that due to technological progress, a number of organizations whose main activity is the provision of Big Data services have entered the business fabric. This study is divided into three major parts: in the first of them, we will address the concept of Big Data and the characteristics that make this technology so unique, in order to understand the reason why it has become the fundamental tool of companies international that are dedicated to the provision of services are data processing; the second part is dedicated to the legal implications of Big Data susceptible to problems of private international law (data protection, legal protection of the algorithm and database, contractual relationships and labour relations in which technology is used Big Data); and, finally, the third part, taking into account the possible problems that may arise and the contractual and non-contractual responsibility that may be generated by the use of Big Data technology, we consider it of great importance to address issues related to international judicial competence and the determination of the applicable law.

Palabras clave / Keywords:

Big Data / Derecho Internacional Privado / Protección de datos / Competencia judicial internacional / Ley aplicable.

Big Data / Private International Law / Data protection / International jurisdiction / Applicable law.

1. ¿Qué es el *Big Data*?

1.1. Concepto

La sociedad está inmersa en una constante digitalización, no solo social, sino también económica e industrial[1]. El ascenso de nuevas tecnologías tales como las redes sociales, el *Cloud Computing,* o el *Internet of Things*, además de la aparición de los dispositivos inteligentes lleva consigo un aumento exponencial del volumen de datos generados que, a su vez, otorgan una

[1] *Vid*. Hua Tan, K. / Ji, G. / Peng Lim, C. / Tseng, M.-L., "Using big data to make better decisions in the digital economy", *International Journal of Production Research*, Núm. 17, Vol. 55, 2017, p. 499.

valiosa información a quien los trata. Esta nueva "sociedad del dato" es el resultado del ascenso del *Big Data*.

Este nuevo concepto constituye un concepto básico y fundamental en la tecnología de la información debido al uso que empresas, ya sean tecnológicas o no, dan para potenciar o reestructurar su modelo económico sobre la base de los datos. Pero, es imposible concebir el concepto *Big Data* como una figura autónoma respecto a otros conceptos tecnológicos, como es el caso del *Internet of Things*, que consiste en una combinación de sensores métricos que permiten captar un gran volumen de datos. De ahí tal concepción intrínseca entre ambos conceptos.

La relación del *Big Data* con otras tecnologías no acaba ahí, pues toma un significado adicional con el auge de las redes sociales, puesto que cualquier comentario, *like*, o valoración hecha en Twitter, Facebook, YouTube, o en cualquier red social constituye una información, un dato, al fin y al cabo. También tiene una gran relación con el *Cloud Computing*, puesto que esos datos, una vez recabados, son almacenados en servidores con unas capacidades de almacenamiento sobredimensionadas, diseñadas específicamente para este cometido.

Big Data, en español, puede ser traducido de varias maneras, por ejemplo, y de forma literal, como "grandes datos", o de una forma más correcta a nuestro entender y en el entorno de las tecnologías de la información, como "macrodatos"[2]. Este nuevo término ha sido adoptado para hacer referencia a la manipulación de un gran volumen de datos, y aunque demos especial importancia a una de las características principales del *Big Data*, como es el volumen, no debemos olvidar que esa ingente cantidad de datos generada proviene de diversas fuentes, que otorgan una gran diversidad cualitativa de datos. Es por ello que otra de las características principales del *Big Data* es la variedad.

Esa cantidad inmensa de datos de diversa calidad suelen fluir en tiempo real. El *Big Data* analiza los datos en tiempo real, por lo que el análisis de datos de hace unas horas o, incluso, de hace unos minutos, puede arrojar resultados no apropiados al fin que buscamos con el *Big Data.* Tan fundamental es la velocidad, que este término es el último de los tres conceptos principales que conforma el *Big Data*, los cuales se les han añadido nuevas

[2] *Vid*. Tascón, M. / Coullaut, A., *Big Data y el Internet de las Cosas. Qué hay detrás y cómo nos va a cambiar*, Ed. Catarata, Madrid, España, 2016, p. 12.

características complementarias debido a la rápida evolución de su práctica, y que posteriormente analizaremos pormenorizado.

Consecuencia del gran número de elementos que conforman el *Big Data,* encontrar una definición que explique de forma rigurosa qué es el *Big Data* es complicada[3]. Aunque podemos encontrar autores que se han atrevido a aportar alguna definición relativamente formal, como la que muestra Starmans, que lo define como "muchos, o demasiados datos de lo que solemos usar, o los cuales no pueden ser manejados, accedidos, analizados, interpretados y validados por medios convencionales, como base para obtener información útil y conocimiento confiable"[4].

Joyanes Aguilar comparte la misma opinión en cuanto a la gran complejidad para encontrar una definición que explique a la perfección qué es el *Big Data*. El mismo autor, habida cuenta de ello, destaca que la concepción del *Big Data* varía según la importancia que el autor dé sobre una característica concreta. Podemos ver así que algunas de las empresas pioneras y punteras a nivel mundial sobre el *Big Data* destaquen el volumen generado de los datos (la cantidad de datos obtenidos), como McKinsey Global Institute[5], o Deloitte[6]; otras la variedad (tipos de fuentes de datos no estructurados, como la interacción social, video, audio, o cualquier cosa catalogable en una base de datos)[7], como Gartner[8], o la velocidad (de creación y utilización) como IDC[9].

No todos los autores otorgan definiciones centradas en sus características. El *Big Data* es visto también desde perspectivas que llegan a trascender

---

3 *Vid*. Mayer-Schönberger, V. / Cukier, K., *Big Data. A Revolution That Will Transform How We Live*, Ed. Houghton Mifflin Harcourt, New York, Estados Unidos de América, 2013, p. 6.

4 *Vid*. Starmans. J.C.M.R., "The Advent of Data Science: Some Considerations on the Unreasonable Effectiveness of Data", Bühlmann, P. / Drineas, P. / Kane, M. / Van der laan, M., *Handbook of Big Data*, CRC Press, Boca Raton (Florida), Estados Unidos de América, 2016, p. 6.

5 *Vid*. McKinsey Global Institute, *op. cit.* p. 6.

6 *Vid*. Deloitte, "Big Data, Big Brother? Striking the right balance with privacy", 2015, p. 4.

7 *Vid*. Joyanes Aguilar, L., *op. cit.* p.19.

8 *Vid*. Elias, H., "El desafío de *Big Data*: Cómo desarrollar una estrategia ganadora", CIO, julio 2012. Disponible en: https://cioperu.pe/articulo/10442/el-desafio-de-big-data-como-desarrollar-una-estrategia-ganadora/ [Última consulta: 30 de agosto de 2019].

9 *Vid*. European Commission, "Worldwide Big Data Technology and Services 2012-2015 Forecast", *IDC Report*, marzo, 2012, p. 1. Disponible en: https://ec.europa.eu/digital-single-market/en/news/worldwide-big-data-technology-and-services-2012-2015-forecast [Última consulta: 30 de agosto de 2019].

los datos y buscan destacar elementos más pragmáticos que las propias características (o uves) por las que fundamental el *Big Data*[10]*:*

1) El *Big Data* como tecnología. Orientada fundamentalmente al desarrollo tecnológico, los usuarios de estas tecnologías vieron la necesidad de diferenciarse de las demás tecnologías existentes hasta la fecha, por lo que crearon este concepto como una "nueva tecnología";

2) El *Big Data* como aplicación. Esta definición enfatiza en las diferentes aplicaciones basadas en los diferentes tipos de *Big Data*. Puede ser definida como una aplicación de procesamiento mediato de datos de la información generada por personas y generadas por máquinas;

3) El *Big Data* como fuente de señales. Es una concepción orientada al *Big Data* como aplicación, pero se centra en el *timing* más que en la variedad de los datos. Se busca que los datos creen una previsión respecto a una situación, o un nuevo patrón respecto del conjunto de datos;

4) El *Big Data* como oportunidad. *El Big data* surge por los avances tecnológicos, cuando años atrás no se podía acceder a ello por la tecnología existente en ese momento; por lo que las bases de datos de las empresas cobraron un sentido tras la llegada del *Big Data*;

5) El *Big Data* como metáfora. Es definido como un proceso de pensamiento humano, una extensión del cerebro humano, al tener como objetivo crear un sistema nervioso propio para el planeta;

6) El *Big Data* como nuevo término para las viejas cosas. En contraposición a la segunda definición, se considera que los proyectos actuales podían hacerse con la tecnología anterior, sin tener que acudir al renombramiento de aquellas con *Business Intelligence* o *Big Data Analytics*.

Tampoco debemos olvidarnos de que el *Big Data* requiere de los elementos materiales necesarios para llevar a cabo su aplicación. Estos son,

[10] *Vid*. Buyya, R. / Calheiros, R. / Vahid Dastjerdi, A., *Big Data: Principles and Paradigms*, Elsevier, Amsterdam, Países Bajos, 2016, p. 10.

los sistemas informáticos, y no cualesquiera. Puyol Montero incluye a tales medios en la concepción del *Big Data*[11].

Una vez analizados los elementos que, unidos todos ellos, conforman el *Big Data*; podemos definirlo como "el análisis de macrodatos de calidades variadas derivados de diversas fuentes que fluctúan a gran velocidad mediante los sistemas informáticos adecuados, con el objetivo de obtener un valor añadido en los productos ofrecidos".

1.2. Características: las V's

Las características del *Big Data* están conformadas por las "uves", que vienen a ser uno de los rasgos más representativos del *Big Data.* Hemos observado que inicialmente se basaban en tres características o "uves", pero con la evolución del *Big Data*, dichas características se han quedado cortas a la hora de afianzar lo que es el *Big Data*. Debido a su expansión, las características se han ido agrupado en *domains* o dominios, que podemos definirlos como sectores especializados de un determinado campo.

El primer conjunto de características clásicas están agrupadas en el llamado *Data domain*[12]. En los albores de su entendimiento, se consideraban que las características del *Big Data* eran:

- Velocidad: se refiere a la velocidad de adquisición de datos y su procesamiento, la velocidad a la que fluyen los datos. El *Big Data* añade un plus de velocidad que permite acelerar el proceso.

- Volumen: la cantidad masiva de datos generados y guardados por las empresas. Tal es la información que tiene que ser medida en petabytes o incluso, exabytes.

---

[11] *Vid*. Puyol Montero, J., *Aproximación jurídica y económica al Big Data*, Ed. Tirant lo Blanch, Valencia, España, 2016, p. 286.

[12] *Vid*. El *Data domain* está basado en la categoría del dato, consistente tanto en una lista enumerada de valores determinados, como un conjunto de normas con restricciones específicas en los valores dentro de esa categoría de datos. Un ejemplo sería atribuir en una tabla de una base de datos una columna destinada al "género". A esta columna se le atribuye uno o dos "códigos valores"; en este caso, "M" para masculino, y "F" para femenino. Por lo tanto, el *Data domain* para la columna de género será "M", "F". *Vid*. Loshin, D., *Enterprise Knowledge Management: The Data Quality Approach*, Ed. Morgan Kaufmann, San Diego (California), Estados Unidos de América, 2003, p. 302.

- Variedad: consiste en los dinámicos y crecientes fuentes de obtención de datos. Las fuentes pueden ser datos de sensores, audio, videos, tráfico online, y muchos más tipos. Los datos pueden venir de forma estructurada, semi-estructurados o no estructurados[13].

Estas tres características se interrelacionan. Así, el volumen de datos se relaciona directamente con la variedad de las diferentes fuentes, a lo que la velocidad del flujo de datos se relaciona con el volumen de datos y la variedad de sus fuentes. En el *Data domain*, la característica determinante es el "volumen". La cantidad de datos siempre es mayor que su variedad o su velocidad.

Posteriormente, el modelo primitivo fue ampliado sucesivamente con nuevas "uves", añadiéndose como características el valor, la visibilidad, el veredicto, la veracidad, la validez, y la variabilidad[14]; derivadas todas ellas de las nuevas perspectivas que otorga el *Business Intelligence domain* y el *statistic domain*.

Las características aportadas por el *Business Intelligence domain*[15] son:

- Valor: ¿los datos recogidos tienen información valiosa para mis necesidades empresariales? Es la pregunta que se busca responder. Es uno de los aspectos críticos en el caso del *Big Data*. No tiene sentido la recolección de todos los datos a menos que seamos capaces de generar algún valor fuera de ella.

- Visibilidad: los datos pueden ser recogidos, seleccionados y procesados; pero para llevar a la práctica un efectivo uso del *Big Data* los datos deben ser presentados de una manera accesible y entendible para encontrar patrones de datos con el objetivo de crear una línea de trabajo sobre ellos.

- Veredicto: es la potencial elección o decisión que debe ser realizada por el tomador de decisiones basado en la amplitud del problema,

---

13 *Vid*. Jain, V. K., *Big data and Hadoop*, Khanna Publishing, New Delhi, India, 2017, p. 4.

14 *Vid*. Buyya, R. / Calheiros, R. / Vahid Dastjerdi, A., *op. cit.,* pp. 10-14.

15 Es el conjunto de metodologías, aplicaciones, prácticas y capacidades enfocadas a la creación y administración de información que permite tomar mejores decisiones mediante la creación de modelos predictivos a los usuarios de una organización. En este sentido, *Vid*. Conesa Caralt, J. (Coord.) / Curto Díaz, J., *Introducción al Business Intelligence*, Ed. UOC, Barcelona, España, 2012, p. 18.

la disponibilidad de los recursos, y su capacidad computacional. Este último valor es el más difícil de cuantificar.

En este *domain*, la característica clave es la visibilidad. Si los datos no son lo suficientemente visibles, no podemos darles valor; en consecuencia, tampoco seremos capaces de tomar una decisión meridianamente segura.

El último sector lo conforma el *statistic domain*. Las siguientes características deben establecer los modelos estadísticos basados en la hipótesis correcta (¿Qué pasaría si…?), que es la fiabilidad de los conjuntos de datos y la fiabilidad de las fuentes de datos. Si la hipótesis es inadecuada o la fuente de datos está contaminada o el modelo estadístico es incorrecto. El análisis llegará a una conclusión incorrecta.

- Veracidad: la veracidad deriva en respuesta a los problemas de la calidad y de fuentes de datos que las empresas empezaban a encontrarse al crear iniciativas con *Big Data*[16].

- Validez: se trata de verificar la calidad de los datos siendo lógicamente sólidos. Enfatiza la precisión de los datos y la evasión de prejuicios.

- Variabilidad: trata con la inconsistencia en la velocidad de la carga de datos en las bases de datos; dicho de un modo más sencillo, la variabilidad se refiere a la variación en las tasas de flujo de datos.

La característica clave de este aspecto es la veracidad, que enfatiza en cómo construir un modelo estadístico cercano a la realidad.

1.2.1. Tipos de *Big Data*

Los datos se clasifican en tres tipos[17]:

1) Datos estructurados: hace referencia a todo dato que puede ser recabado mediante una base de datos *SQL*[18] con filas y columnas. Tienen clave relacional y pueden ser asignados fácilmente en los campos prediseñados. Los datos estructurados dependen de crear un dato

[16] *Vid*. Zikopoulos, P. C., *Harness the power of big data, the IBM Big data platform*, Ed. McGraw-Hill, New York, Estados Unidos de América, 2013, p. 9.
[17] *Vid*. Jain, V. K., *Big data and Hadoop*, *op. cit.,* p. 12.
[18] *SQL* (*Structure Query Language*) es un lenguaje de programación creado para manejar y ordenar datos en sistemas de bases de datos relacionales.

modelo. Un modelo de los diferentes datos que necesita una empresa que serán recolectados, y cómo serán almacenados, procesados y accedidos aellos. Esto implica también definir qué campos de datos serán almacenados y cómo ese dato será almacenado: tipo de dato (numérico, divisa, alfabético, nombre, fecha, dirección) y cualquier restricción en la entrada de datos (número de caracteres; restricción a ciertos términos –valores– como "M", "F"; o "D", "Dña")[19].

2) Datos semi-estructurados: es información que no reside en una base de datos relacional, pero que tiene determinadas propiedades organizativas que lo hacen fácil de analizar. Con determinados procesos, pueden llegar a incluirse en una base de datos relacional.

3) Datos no estructurados: se refiere a la información que no tiene predefinido un dato modelo, o no está organizado de una manera predefinida. La información no estructurada suele ser textos con una alta densidad de contenido, pero puede contener datos tales como fechas, números, y hechos también. Esto deriva en irregularidades y ambigüedades que lo hacen difícil para comprender el uso de programas tradicionales como comparación con datos almacenados en forma de ficheros en bases de datos, o anotados en documentos.

Técnicas como la minería de datos o el procesamiento de lenguajes naturales y la analítica de texto proporcionan diferentes métodos para encontrar patrones en esa información; o de otra forma, interpretarla.

Ejemplos de datos no estructurados son los libros, periódicos, documentos, metadatos, audio, video, dato analógico, imágenes, ficheros, y texto desestructurado como el cuerpo de un mensaje de correo electrónico, una página *web*, o un procesador de texto. Los datos no estructurados son los más numerosos. Se estima que el 80% de los datos que posee una empresa no están estructurados. Los datos no estructurados están por todas partes. Estos pueden ser generados tanto por una máquina como por una persona.

1) Como ejemplos de datos no estructurados generados por una máquina:

[19] Los datos que concurren al rellenar un formulario de google son datos estructurados; puesto que son ordenados en un soporte que facilita la creación de una base de datos relacional, cuando ligamos la pregunta a la respuesta que damos.

a. Imágenes por satélite, que incluyen los datos meteorológicos, o los datos generados por los satélites de vigilancia.

b. Datos científicos: imágenes sísmicas o datos atmosféricos.

c. Fotografías y videos: respecto a seguridad, vigilancia, y tráfico.

d. Datos de radares o sonares: datos de vehículos, meteorológicos, y perfiles sísmicos–oceanográficos.

2) Como ejemplos de datos generados por humanos:

a. Textos internos de una empresa: logo, *e-mails*, encuestas, resultados, etc.

b. Datos de los *social media*: datos generados de webs con fuerte contenido social como YouTube, Facebook, Twitter, LinkedIn, y Flickr.

c. Datos móviles: mensajes de texto, localización, tráfico online, etc.

d. Contenido *web*: proviene de cualquier sitio con un contenido deliberadamente no estructurado, como YouTube, Flickr, o Instagram.

1.3. Clasificación de datos

Los datos se pueden clasificar en: a) estructurados, b) semi-estructurados y c) no estructurados; ahora bien, esos datos se pueden clasificar también según la fuente de la que procedan. Soares realiza una clasificación de estas fuentes[20]:

1.3.1. Web y social media

Consiste en contenido Web, y en la información obtenida por las redes sociales como Facebook, Twitter, LinkedIn y demás redes. Estos datos se capturan, almacenan y distribuyen dependiendo de su sub-origen: los datos

[20] *Vid*. Soares, S., "Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today", *Big Data Governance. An Emerging Imperative*, Ed. MC Press, Boise (Idaho), Estados Unidos de América, 2012, pp. 7-8. Disponible en: https://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/ [Última consulta: 30 de agosto de 2019].

generados en las redes sociales como consecuencia de determinadas acciones realizadas en éstas (*clicks*, *tweets*, *retweets*, y demás entradas en Twitter; entradas en Tumblr, *posts* de Facebook); sistemas de contenidos *web* como YouTube o Flickr, y sitios de almacenamiento de información (Cloud) como Dropbox, Box.com, SugarSync u OneDrive.

1.3.2. Machine-to-machine data

Máquina-a-máquina (M2M) se refiere a tecnologías que permiten que tanto los sistemas inalámbricos como los cableados se comuniquen con otros dispositivos. M2M utiliza un dispositivo como un sensor o un medidor para capturar un evento (como velocidad, temperatura, presión, flujo o salinidad) que se transmite a través de una red inalámbrica, cableada o híbrida a una aplicación que traduce el evento capturado en información relevante. Las comunicaciones M2M crean el llamado "Internet de las cosas".

1.3.3. Grandes transacciones de datos

Esto incluye las demandas de atención médica, registros de detalle de llamadas de telecomunicaciones y registros de facturación, reclamaciones de consumidores. Los grandes datos de transacciones están cada vez más disponibles en formatos semi-estructurados y no estructurados.

1.3.4. Biometría

La información biométrica incluye huellas dactilares, reconocimiento de voz, escáneres de retina e iris, reconocimiento facial y genético. Los avances tecnológicos han aumentado enormemente los datos biométricos disponibles. La aplicación de la ley, el sistema legal y las agencias de inteligencia han estado usando esta información por mucho tiempo. Sin embargo, los datos biométricos están cada vez más disponibles en el ámbito comercial donde se puede mezclar con otros tipos de datos como los medios de comunicación social, lo que hace aumentar el volumen de datos generados por los biométricos.

1.3.5. Datos generados por humanos

Los seres humanos generan grandes cantidades de datos tales como notas de los agentes del centro de llamadas, grabaciones de voz, correo

electrónico, documentos en papel, encuestas y registros médicos electrónicos. Estos datos pueden contener información sensible que debe ser enmascarada. Puede contener ideas que pueden mejorar la calidad de los conjuntos de datos estructurados y deben integrarse con MDM (*Mobile Device Management*).

2. Implicaciones legales del *Big Data* susceptibles de problemas de Derecho Internacional Privado

2.1. Implicaciones para la protección de datos

Debemos destacar la incidencia en uno de los elementos fundamentales del derecho a la protección de datos: el consentimiento. Si la utilización de las herramientas del *Big Data*, comprende la interrelación de grandes bases de datos y la cesión o comunicación de datos de carácter personal entre ellas, esto exige el consentimiento específico, libre, inequívoco e informado del titular de los datos. Teniendo en cuenta que este consentimiento no puede ser recabado genéricamente y, mucho menos, para grandes volúmenes de datos que se encuentran desestructurados en diferentes almacenamientos y entornos de acceso telemático, la dificultad de su utilización lícita resulta evidente[21].

Mención especial debemos hacer a uno de los efectos con más impacto a raíz del *Big Data*: la elaboración de perfiles.

La elaboración de perfiles comprende la salida del proceso algorítmico automatizado, e implica el reconocimiento de patrones para propósitos predictivos o de evaluación basados en datos voluntarios, observados y obtenidos en la nube[22].

Un perfil implica encuadrar a una persona, en función del resultado del tratamiento informatizado de sus datos, en un grupo concreto al que se le atribuyen unos comportamientos futuros, cuya utilización en la toma de decisiones puede suponer una valoración desfavorable de sus características y, por consiguiente, su discriminación en varios actos de su vida[23]. Es por ello

[21] *Vid*. Davara Rodríguez, M. A., "Big Data", *El Consultor de los Ayuntamientos,* Núm. 15, Ed. Wolters Kluwer, Madrid, España, 2013, p. 1.

[22] *Vid*. Savirimuthu, J., "Do algorithms dream of 'data' without bodies?", *International Review of Law, Computers & Technology*, Núm. 2, Vol. 31, 2017, p. 256.

[23] *Vid*. Garriga Domínguez, A., *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, España, p. 67.

que los perfiles suponen un impacto en los derechos de los afectados por la gran cantidad de datos recogidos y utilizados para elaborarlos, combinando y cruzando los distintos datos recogidos por varias vías[24]. Esos datos por los cuales se basan para la creación de perfiles suelen ser enfermedades que padecimos o padecemos actualmente, accidentes de tráfico que hemos sufrido, deudas pasadas y presentes, y una de sus principales manifestaciones es la creación de "listas negras"[25], con graves efectos negativos sobre los individuos tanto en el entorno asegurador, como en el crediticio.

Debido a los problemas resaltados, el Comité de Ministros del Consejo de Europa adoptó el 23 de noviembre de 2010 la Recomendación (2010)13 sobre la protección de las personas físicas con respecto al tratamiento automatizado de datos de carácter personal. En la recomendación reconocen los usos del *Big Data* como medio para recopilar y tratar datos a gran escala tanto en el sector público como en el privado, además de mejorar y segmentar el mercado en busca de mayores beneficios y en la prevención de conductas fraudulentas; pero también resalta los problemas derivados de su uso:

a) La creación de perfiles puede conducir a incluir a las personas en categorías predeterminadas sin que tengan conocimiento de ello. La falta de precisión por el tratamiento automatizado puede suponer graves riesgos para los derechos y libertades.

b) La atribución de perfiles puede generar datos personales no proporcionados por el afectado, viéndose afectado el control sobre la identidad de la persona interesada, y siendo privada de manera arbitraria del acceso a ciertos bienes y servicios, violando el principio de no discriminación.

Es por todos los riesgos presentados por el que existe el derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado en las diferentes normas sobre protección de datos europeas. El nuevo Reglamento General de Protección de Datos (en adelante, RGPD) materializa este derecho en el artículo 22 estableciendo que el afectado tendrá derecho a no ser objeto de tales conductas cuando le afecten jurídicamente o tengan un efecto similar. Este derecho es diferente a otros que podemos encontrar en

[24] *Vid*. Sánchez Bravo, A. (Ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez*, Ed. Punto Rojo Libros, Sevilla, España, 2014, p. 18.

[25] *Vid*. WP 65 Documento de Trabajo sobre las listas negras. Adoptado el 3 de octubre de 2002.

el RGPD, como el derecho de oposición (artículo 21), el derecho de supresión (artículo 17), o el derecho a la rectificación (artículo 16), puesto que este derecho puede parecer que no se ejerce por parte del afectado. Esta misma disposición puede dividirse teóricamente en dos vertientes: por un lado, el apartado 1 es configurado como un "derecho" del afectado a que cualquier decisión que pueda tener efectos jurídicos exista intervención humana; y por el otro, el apartado 4 establece la "prohibición" de que las decisiones automatizadas no se basen en categorías especiales datos.

Dependiendo de cómo se tratase, las consecuencias pueden ser varias[26]:

1. Tratándolo como un derecho[27] de oposición hace depender su efecto de la acción de la persona afectada, al menos para los procesos de decisión que no entran dentro de las tres categorías de excepciones del párrafo segundo. Este es claramente un resultado más débil de una perspectiva de privacidad y protección de datos que si el artículo 22.1 es tratado como una prohibición.

2. Considerándolo una prohibición, se prohíben aquellos procesos de decisión que no estén comprendidos en las excepciones previstas en el apartado 2, independientemente de la acción o inacción de la persona afectada, permitiendo únicamente los procesos decisorios especificados en el apartado 2 (con las calificaciones indicadas en los párrafos tercero y cuarto). Tal resultado es mejor respecto al objetivo general del artículo 22 y, de hecho, del RGPD en general: proteger la privacidad y la protección de datos como derechos humanos fundamentales frente a la evolución tecnológica y de cualquier otro tipo.

2.2. Implicaciones en la protección legal del algoritmo y la base de datos

Las conclusiones son el resultado de la aplicación concreta de los datos obtenidos a modelos y patrones derivados de esos datos. Esos patrones son hallados mediante la aplicación de un algoritmo específico (eso es, de un conjunto ordenado de operaciones sistemáticas para hacer un cálculo y obtener una solución). Los algoritmos son "procesos lógicos formados por una serie de instrucciones o reglas que permiten resolver problemas partiendo de unos datos de entrada, mediante la obtención de unos datos

[26] *Ibídem*, p. 10.

[27] A favor de esta consideración, *vid*. Savirimuthu, J., "Do algorithms dream of 'data' without bodies?", *op, cit.* p. 259.

de salida"[28]. Los algoritmos son codificados por un programador en un lenguaje algorítmico antes de ser traducidos a una secuencia binaria legible por máquina. El lenguaje algorítmico es un lenguaje especialmente diseñado para expresar cálculos matemáticos o simbólicos y así expresar operaciones algebraicas en una notación, que recuerda a la lógica y está relacionada con la matemática[29]. El algoritmo es el paso intermedio entre la recolecta masiva de datos y su aplicación práctica.

En cuanto a la protección legal del algoritmo, se ha mostrado complicada su defensa legal:

a. Patentes. en el ámbito nacional, está descartado su patentabilidad debido a su consideración como mero método matemático por el artículo 4.4 de la Ley 24/2015 de Patentes[30][31]. Respecto al ámbito europeo, también se rechaza su patentabilidad por los mismos motivos en el artículo 52 del Convenio de Múnich. La cámara de recursos de la Oficina Europea de Patentes ha rechazado varías solicitudes de patente de algoritmos[32].

b. Propiedad intelectual. Aunque podemos encuadrar como software un algoritmo, el artículo 96.4 del TRLPI no protege "las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces". En este sentido, se ha pronunciado el TJUE en el asunto C-406/2010 *SAS Institute Inc. vs. World Programming Ltd*[33].

c. Secreto industrial o comercial/*Know-How.* Como última vía frente a las anteriores, el *Know-How* puede ser una solución adecuada. Su definición no se encierra recogida legalmente, sino que ha sido

[28] *Vid*. González Royo, I. / Pina, C., "¿Cómo se protegen legalmente los algoritmos?", *Diario La Ley*, núm. 8776, 2016, p. 1.

[29] *Vid*. Vedder, A., "Accountability for the use of algorithms in a big data environment", *International Review of Law, Computers & Technology*, Núm. 2, Vol. 31, 2017, p. 210.

[30] BOE-A-2017-3550.

[31] El Real Decreto 316/2017, de 31 de marzo, por el que se aprueba el Reglamento para la ejecución de la Ley 24/2015 tampoco ofrece novedades respecto a esta materia.

[32] Vicom Systems Inc. (1986); IBM (1989); Pension Benefit System Partnership (2000); Infineon Technologies AG (2006).

[33] "[N]i la funcionalidad de un programa de ordenador ni el lenguaje de programación o el formato de los archivos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones constituyen una forma de expresión de ese programa y, por ello, carecen de la protección del derecho de autor sobre los programas de ordenador en el sentido de la Directiva 91/250".

el Tribunal Supremo, en su STS de 19-12-2002 quien la ha definido como "conjunto no divulgado de informaciones técnicas, patentadas o no, que son necesarias para la reproducción industrial directamente y en las mismas condiciones, de un producto o un procedimiento". La protección del *Know-How*, como secreto industrial, está recogido en la Ley de Competencia Desleal[34], y en el Código Penal (artículos 278 y ss.).

Respecto a las bases de datos, gran parte del valor de las empresas que se utilizan el *Big Data* basan sus activos en los datos que van acumulando y organizando en bases de datos para su análisis. En un primer lugar, podría aplicarse el régimen de protección que brinda nuestra Ley de Propiedad Intelectual (LPI)[35].

a) Protección de la base de datos por el derecho de autor. Es la protección otorgada por el artículo 12 LPI. Es bastante complicada de obtener, pues la ley exige que la base de datos sea original en cuanto a la estructura y la disposición de sus contenidos (12.1 LPI). Los datos producidos o recogidos por las empresas no son susceptibles de protección como bases de datos en atención al régimen de los derechos de autor. La razón es que dichos datos son recopilados y procesados de manera automática. No existe una intervención humana que pueda ser considerada una creación intelectual en la organización y recolección de los materiales incorporados a la base de datos[36].

b) Protección de la base de datos por el derecho *sui generis,* respecto de su contenido, impidiendo la extracción y la reutilización. Es la protección más usual, encaminada a la protección de la inversión en

[34] "Artículo 13. Violación de secretos. 1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14. 2. Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo. 3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto".

[35] *Vid*. Vivas-Tesón, I., "La tutela `sui generis´ de las bases de datos", *Revista de Derecho Patrimonial*, Núm. 21, 2008; González Royo, I., "La protección de los intangibles intelectuales e industriales en el contexto del Fintech", *Diario La Ley*, Núm. 8795, 2016.

[36] STJUE de 1 marzo 2012, C-604/10, *Football Dataco I*.

la creación de la base de datos, pues impide que se pueda extraer y reutilizar su contenido sin autorización del titular. El régimen de esta protección se encuentra en los artículos 133-136 LPI, y cuyo régimen se debe a la transposición de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. Tampoco podría aplicarse dicha protección. En este caso, el problema es que la protección se concede a la inversión sustancial en la obtención de los datos, pero no en su producción. En este sentido, el TJUE, en la sentencia de 9 noviembre 2004, C-444/02, "Fixtures Marketing".

Esta protección corresponde al fabricante de la base de datos (persona física o jurídica que realiza la inversión) y se extiende durante quince años desde la elaboración o divulgación de la misma, con posibilidad de obtener una protección adicional por ese plazo en caso de realizarse una nueva modificación sustancial de la misma. Es muy importante probar la inversión que se ha hecho, no en la creación de los datos, sino en la organización y disposición de los mismos, como viene señalando el TJUE[37].

La Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas[38], permite aumentar el nivel de protección de los secretos comerciales. La Directiva define al *Know-How* en su Considerando 1 como "obtención, desarrollo y aplicación de conocimientos técnicos". Para que se considere "secreto comercial" a efectos de la Directiva, debe reunir determinados elementos:

1. Ser secreta, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas,

2. Tener un valor comercial ya sea real o potencial, precisamente por ser secreto, y

[37] SSTJCE de 9 de noviembre de 2004 (asuntos C-46/02 (TJCE 2004, 320), C-203/02 (TJCE 2004, 321), 338/02 (TJCE 2004, 319) y 644/02 SIC (TJCE 2004, 318).
[38] DOUE L 157/1 de 15 de junio de 2016.

3. Haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control.

Teniendo en cuenta estas características, podemos afirmar que los algoritmos y las bases de datos pueden considerarse como secretos comerciales, y estar protegidos tanto por la Directiva como por la Ley de Competencia Desleal.

2.3. Implicaciones legales en las relaciones contractuales

El *Big Data* interesa al Derecho internacional privado por una simple razón, los prestadores de servicio de procesamiento de la información normalmente se encuentran en países distintos al del origen de la información recogida, consecuencia directa del *Cloud Computing*, esta tecnología permite, el almacenamiento, el tráfico y el tratamiento a través de internet, mediante servidores de almacenamiento de datos interconectados por todo el globo, de forma que es fácil que puedan surgir litigios jurídicos internacionales**.** Además, debemos añadir, que la información almacenada en un país distinto al titular de los datos, tiende a fluctuar de un lugar a otro, produciéndose así un tráfico masivo de los datos a través de las fronteras.

Al hilo de lo anterior inexorablemente se crean una serie de relaciones jurídicas que tienen importancia para el Derecho Internacional Privado.

Y la cuestión es ¿por qué esta normativa afecta a la tecnología *Big Data*?, en primer lugar, porque como su propio nombre indica, la materia prima de esta tecnología son los datos, en segundo lugar, porque la mayoría de esos datos son obtenidos de personas físicas y, en tercer lugar, porque la tecnología *Big Data* es la herramienta principal de aquellas empresas que prestan servicios de almacenamiento y tratamiento de datos o que simplemente en su tráfico habitual empresarial almacenan datos personales.

Consecuencia directa del almacenamiento y tratamiento que afecta a las relaciones que surgen entorno al *Big Data*, está la obligación de diligencia por parte del empresario que participa en el tratamiento de datos, diligencia que se traduce en la armonización del *Big Data* con la privacidad[39]. Dicha diligencia se cristaliza en las empresas a través de la inclusión en el contrato de cláusulas de protección de datos o cláusulas de privacidad y confidencialidad.

[39] *Vid*. Díaz Granados Ordoñez, G. F., "La comercialización del *Big data and commercial* law", *Univ. Estud. Bogotá*, núm. 14, Julio-Diciembre 2016, pp. 11-128.

El fundamento de la inclusión de dichas cláusulas es el fortalecimiento de la privacidad y el derecho a la protección de datos a nivel mundial.

La tecnología *Big Data* es un fenómeno reciente que ha provocado la aparición de empresas dedicadas a esta actividad, las cuales, se han convertido en parte de las relaciones contractuales. Pues bien, como esta tecnología abarca una actividad extremadamente amplia, las empresas ubicadas dentro del *Big Data*, pueden, tan solo, dedicarse a una parte del proceso. En este sentido nos podemos encontrar empresas que solo se dedican a recoger y almacenar la información, empresas que se dedican al procesamiento y análisis de los datos e incluso empresas que se dedican a la compra-venta de datos. Consecuencia de ello, tanto los Estados como el legislador europeo han visto la necesidad de elaborar normas que regulen la forma en que utilizan los datos procesados, así pues, estas empresas deberán elaborar contratos que sean compatibles con la normativa, para no incurrir en un tratamiento ilícito de datos respecto de sus titulares.

En lo referente a las relaciones contractuales en esta materia, encontramos: a) por un lado, la empresa que forma parte de alguna de las etapas del *Big Data* y que presta un servicio relacionado con el almacenamiento o tratamiento; y, por otro lado, el otro sujeto que interviene puede ser otra empresa que contrata sus servicios o, también un usuario y consumidor. A su vez, cuando se trata de una empresa que contrata el servicio de una prestadora de servicios de *Big Data*, tendrá que establecer relaciones contractuales y legitimar los datos que transfiere, cuando el titular de dichos datos son terceras personas, como por ejemplo clientes o trabajadores.

Algunos casos de empresas prestadoras de servicios que utilizan tecnología *Big Data* podrían ser:

* Un ejemplo de estas relaciones sería la empresa que contrata a otra empresa prestadora de servicios de *Big Data,* como es el caso de la empresa estadounidense Opta Sports[40], una empresa dedicada a recoger y analizar datos deportivos. Esta empresa ha convertido el dato deportivo en un bien mercantil, su principal función es recoger datos para posteriormente procesarlos obteniendo estadísticas de rendimiento de deportistas o equipos, ofreciendo a las empresas con las que contratan informes reales y eficientes basados en datos reales cuya principal función es aumentar las ganancias

[40] Disponible en: https://www.optasports.com/sports/ [Última consulta: 30 de agosto de 2019].

económicas. Sus principales clientes son empresas como Nike, IBM, Marca, etc.

En este caso tenemos una empresa que contrata los servicios a otra, así vemos como el *Big Data* se convierte en el objeto material de un contrato. Por lo tanto, estamos ante una relación mercantil entre dos empresas, que vendría regulada por la normativa mercantil, en este caso en concreto, atendiendo a la internacionalidad de las empresas se aplicaría el Reglamento "Roma I".

Ante esta situación surge una cuestión importante que debemos puntualizar, en lo relativo a las partes que intervienen en el contrato de prestación de servicios, y es que, en esta relación existe una parte indispensable, los datos que obtiene la prestadora de servicios de *Big Data* en principio no le pertenecen, sino que son titulares terceras personas. Por lo tanto, debe existir un consentimiento de los titulares de los datos, los cuales deben conocer y permitir expresamente dicho tratamiento.

En este sentido, nos encontramos ante una relación triangular, es decir, las personas titulares de los datos, la empresa prestadora de servicios de *Big Data*, y la empresa que adquiere los datos tratados. Estas relaciones deberían estar reguladas por un contrato que legitime el tratamiento, en caso contrario, es decir, que la recogida de datos no se haga con el consentimiento expreso de sus titulares, se podría estar incurriendo en una responsabilidad extracontractual, por un tratamiento ilícito de los datos. Para ver con más claridad la relación entre titular de los datos y la empresa prestadora de servicios tenemos el caso de la empresa Target.

La empresa con sede en Minneapolis (EE.UU.), Target es una de las más importantes cadenas de grandes almacenes de EE.UU., lo que nos interesa de esta empresa es cómo utilizó la tecnología *Big Data* para incrementar la venta de productos para embarazadas. Básicamente lo que hizo fue recopilar toda la información de los hábitos de compra de sus clientas para poder predecir cuales de ellas estaban embarazadas. Detectaron que había un gran porcentaje de mujeres embarazadas que durante las primeras semanas de embarazo tenían hábitos de compra parecidos, se las clasificaba y seguidamente se les enviaba publicidad y cupones de compra de productos para embarazadas.

La forma que tenían para recopilar la información personalizada era a través del pago que hacían estas clientas con las tarjetas de pago que proporciona esta cadena de almacenes.

En este caso vemos un claro ejemplo de cómo una empresa recopila datos y que tras su análisis y procesamiento elabora perfiles de consumidores, para así, discriminar o centrarse en enviar publicidad para poder inferir en los hábitos de compra y modificar su comportamiento.

Entonces ¿hasta qué punto puede una empresa prestadora de servicios de *Big Data* utilizar esa información sin el consentimiento de los consumidores y usuarios?, en este sentido el RGPD otorga una serie de derechos a las personas físicas en cuanto al control de sus datos. Por lo tanto, si una empresa utiliza los datos como así lo hizo Target, debería informar al titular de los mismos del uso que se va a realizar con sus datos y la finalidad de su obtención, y, además ofrecerle canales para ejercitar sus derechos de Acceso, Rectificación, Cancelación y Oposición (en lo sucesivo, ARCO), y todo esto mediante una cláusula, por ejemplo, en el contrato de la obtención de la tarjeta de crédito que las empresas de este sector ofrecen a sus clientes.

2.4. Implicaciones legales en las relaciones laborales

Otra de las áreas en la que se usa la tecnología del *Big Data* es en el ámbito laboral, las empresas usan esta tecnología para recoger datos y, así, por ejemplo, analizar el rendimiento de los trabajadores en determinadas épocas del año. Por este motivo no debemos olvidarnos de las implicaciones legales que existe en el ámbito laboral.

El pasado 25 de mayo de 2018 supuso el fin del proceso de adaptación, consecuencia de ello, todas las empresas deberían haber implantado las nuevas exigencias que establece el RGDP de la Unión Europea (en adelante, UE); es decir, conocer los nuevos derechos que tendrán que proporcionar como responsables de datos ante los interesados propietarios de éstos, así como cumplir con las nuevas obligaciones.

En primer lugar, apuntar, que el trabajador está revestido de todos los derechos que le reconoce el reglamento, es decir, los derechos ARCO, además, de otros complementarios como el de información y el de portabilidad.

Ahora la cuestión es, ¿cuál sería el instrumento que legitima el tratamiento de los datos de los trabajadores? La respuesta la encontramos en la firma del contrato de trabajo siempre que el tratamiento quede dentro de los límites de la propia relación laboral. Con esto, existen determinados tratamientos que no quedan amparados por la firma del contrato y, por lo tanto, su licitud dependerá del consentimiento del trabajador.

A la hora de respetar los límites de la protección de datos en la relación laboral, la empresa deberá tener en cuenta que el RGPD no será la única normativa que la regula, sino que el propio Reglamento deja la puerta abierta a que se incluyan especialidades en convenios colectivos y por las leyes nacionales, por este motivo, la empresa tendrá que tener conocimiento de las obligaciones que establece el RGPD, pero también aquellas especialidades que son objeto de desarrollo en el convenio colectivo que regula su actividad.

A continuación, vamos a ver sucintamente aquellos tratamientos en los que el empresario debe llevar especial cuidado:

a) Cesión de datos del empresario a terceros

En el desarrollo de la actividad empresarial es común la externalización de determinados servicios, que el empresario no quiere o no puede asumir en su propia organización y, el ámbito de las relaciones labores con su personal laboral no es una excepción.

Una conducta muy habitual de cesión de datos del empresario de terceros, sería la que se produce con la externalización de las tareas de contabilidad, es decir, asesorías que se encargan de gestionar los pagos a la seguridad social de los trabajadores, de elaborar las nóminas, gestionar y tramitar incapacidades o accidentes de trabajo, o, como es el caso, a empresas prestadoras de servicios de *Big Data,* también sucede que actualmente las propias empresas tienen un área compuesta por analistas especialistas en *Big Data*.

Pues bien, estas tareas inexorablemente llevan consigo la cesión de los datos personales de los trabajadores.

La cesión de datos del empresario a terceros, requiere el consentimiento del trabajador, con excepción de aquellas cesiones que están legitimadas por una disposición legal, es el caso de los datos que se aportarán a la Tesorería General de la Seguridad Social (TSGG), o la Mutua de Accidentes de Trabajo, etc… En este tipo de situaciones no es necesario el consentimiento del trabajador puesto que es obligación del empresario facilitar dicha información.

Tampoco será necesario el consentimiento cuando se utilicen los datos para la contratación de planes de pensiones o seguros de vida, que la empresa haga en beneficio de sus trabajadores.

En el caso de la subcontratación de asesorías que gestionen la confección de nóminas no será preciso el consentimiento, ya que se entiende otorgado en la firma del contrato de trabajo, aunque se deberá informar al trabajador de tal fin.

Finalmente, en el caso de las contratas o subcontratas, estará permitida la cesión de datos los trabajadores de la empresa subcontratada, a la empresa principal mientras dure la relación empresarial entre empresas, sin embargo, como el caso anterior, los trabajadores deberán ser informados de la identidad de la empresa principal, duración, lugar, etc.

Cualquier cesión que no se produzca al amparo de una norma que lo permita, se considerará un tratamiento ilícito, si no se obtuvo el consentimiento del trabajador.

b) Los datos en el proceso de selección

Aquí nos situamos en el ámbito de las relaciones precontractuales y más concretamente, en aquellos procesos de selección que realiza la empresa directamente, sin intermediar empresas de colocación laboral.

En este sentido habrá que tener las mismas cautelas que en las relaciones contractuales; sin embargo, se entiende lícito el tratamiento de los datos sin consentimiento del interesado para que sus datos sean tratados en procesos de selección y colocación exclusivamente. Dicho consentimiento se entiende otorgado cuando el solicitante envía su currículum a una empresa.

Al hilo de lo dicho anteriormente, podemos distinguir dos fases dentro de las relaciones precontractuales, una de ellas sería el recibimiento del currículum y, la otra la que se produce en el desarrollo del proceso de selección.

Con respecto a la primera, la recepción del currículum se puede producir de varias formas, por ejemplo, la publicación del mismo en redes sociales como puede ser LinkedIn, que sirve como plataforma para poner en contacto candidatos y empresas, y otra opción puede ser el envío del currículum por parte del interesado a la empresa.

En ambos casos se presume que el interesado otorga el consentimiento para el tratamiento de sus datos para los fines de un posible reclutamiento, sin embargo, existen una serie de buenas prácticas empresariales que pueden blindar de mayor seguridad jurídica a dicho consentimiento implícito.

En segundo lugar, y haciendo referencia a la segunda fase, perteneciente al proceso de selección, se trata de una fase en la que la empresa a través de entrevistas, o dinámicas de grupo, trata de recabar información detalla sobre las capacidades candidato, lo que se traduce en la obtención de más datos personales.

En esta fase se deberá informar al candidato que el tratamiento de sus datos personales está destinado exclusivamente al proceso de selección.

c) Los datos de salud

Los datos de salud se consideran datos especiales, son aquellos relativos a la salud física y mental de una persona que revelen su estado de salud.

El responsable del tratamiento de los datos de salud dependerá de si el servicio de reconocimiento médico y de prevención forma parte de la empresa o, por el contrario, se haya contratado un servicio ajeno; en el primer caso el responsable será el empresario, y en el segundo caso, la empresa contratada.

A la vista de las implicaciones legales que tiene la tecnología *Big Data* en los distintos ámbitos expuestos anteriormente, encontramos que es vital elaborar contratos, ya sea entre empresas, entre trabajadores o, entre consumidores o usuarios, con cláusulas que respeten los derechos que les asisten, para así, encontrar el equilibrio entre los intereses de la empresa prestadora de servicios de Big Data y el resto de sujetos.

3. Afectación de las cuestiones legales desde la perspectiva del Derecho Internacional Privado

Destacamos tres cuestiones desde la perspectiva del Derecho Internacional Privado: la protección de datos, la protección del algoritmo y la base de datos.

3.1. Protección de datos

3.1.1. Competencia judicial internacional

En materia de protección de datos, es necesario tener en cuenta el RGPD, en la medida en que su artículo 3 (ámbito de aplicación territorial) facilita el sometimiento a la legislación europea no solo cuando los datos de carácter

personal los traten responsables o encargados con establecimiento en la UE, sino también cuando, sin establecimiento en la UE, traten datos de residentes en la UE relacionados con la oferta de bienes o servicios a esos interesados en la UE.

En este contexto, el artículo 82 del RGPD remite al artículo 79.2 el lugar donde debe dirigirse el afectado derivado de un supuesto de responsabilidad del artículo 82. En este sentido, el artículo 82.6 nos remite al artículo 79.2, el cual dispone que las acciones dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro donde estos tengan un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Como hemos visto, las acciones objeto del artículo 82 tienen un carácter "civil-mercantil", que, a su vez, se encuadran dentro del ámbito de aplicación del artículo 1.1 del Reglamento (UE) 1215/2012 Del Parlamento Europeo y Del Consejo de 12 de diciembre de 2012 "Bruselas I Bis"[41], y cuya materia no está en los supuestos de exclusión del artículo 1.2.

Aunque se dé por hecha la adecuación de esta acción a los supuestos de responsabilidad extracontractual cuando exista un perjuicio relacionado con un tratamiento de datos ilícito según el artículo 82.6 del RGPD; pero es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento "Bruselas I Bis" si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato[42]. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente; aunque la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual.

Concretando más en el fuero del establecimiento del responsable, el artículo 79.2 permite demandar en el Estado miembro en el que el respon-

[41] DOUE L 351/1, de 20 de diciembre de 2012.

[42] SSTJUE de 13 de marzo de 2014, *Brogsitter*, C-548/12; 14 de julio de 2016, *Granarolo*, C-196/15.

sable o el encargado tengan un establecimiento. Como hemos estudiado en el apartado III del presente trabajo, debe tenerse un concepto flexible de "establecimiento", tal y como se indica en la STJUE *Weltimmo* debe extenderse "a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable"[43]. Para ello, debe valorarse también el "grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión". En la STJUE *Amazon EU Sàrl* considera posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado[44], siendo posible considerar como "establecimiento" un representante de la sociedad si actúa con un grado de estabilidad suficiente[45].

De esta consideración se desprende que cualquier establecimiento del encargado o del responsable permite atribuir la competencia a los tribunales del Estado miembro en el que esté sito. Tampoco será necesario que la acción esté dirigida a las actividades de ese concreto establecimiento, sino que la existencia de cualquier establecimiento extiende el daño causado.

El foro alternativo que prevé el RGPD permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual. Para su consideración, será necesario que el afectado tenga un grado de permanencia que revele una situación de estabilidad[46].

La residencia habitual no es un concepto sinónimo al de "centro de intereses de la víctima" que promulga la STJUE *eDate Advertising*[47], que aunque en principio suele coincidir con la "residencia habitual", podemos encontrarlo en otro Estado cuando exista un vínculo particularmente estrecho con ese otro Estado que resulte de otros indicios, como el ejercicio de una actividad profesional. La consideración de este foro de competencia no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño[48].

---

43 Apartados 31 de la STJUE *Weltimmo* y. 75 de la STJUE *Amazon EU Sàrl*.

44 Apartados 76 y 77.

45 Apartado 30 de la STJUE *Weltimmo.*

46 STJUE 22 de diciembre de 2010, C-497/10, *Mercredi* ECLI: EU: C: 2010:829.

47 STJUE C-509/09 y C-161/10 *eDate Advertising* ECLI: EU: C: 2011:685.

48 *Vid*. Orejudo Prieto de los Mozos, P., "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, Núm. 4, 2013, p. 23.

La compatibilidad entre los foros del artículo 79.2 y los del "Reglamento Bruselas" I bis deriva del artículo 67 de este último Reglamento, al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares, como es el caso del artículo 79.2 del RGPD. En cuanto a los argumentos presentados por el RGPD, encontramos el Considerando 147 que afirma que las normas generales de competencia judicial del Reglamento "Bruselas I bis" "deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD". El Considerando 145 estipula que el demandante "deberá tener la opción" de ejercitar las acciones en los tribunales de los Estados miembros.

Observando lo anterior, revela que el RGPD pone a disposición de los afectados la posibilidad puedan utilizar los foros de competencia del artículo 79.2, en contra del inciso imperativo que recoge ese mismo párrafo. Por lo tanto, cabe afirmar que los foros recogidos en el RGPD son complementarios a los recogidos por el Reglamento "Bruselas I bis"[49] que explicamos a continuación:

1. Sumisión expresa (artículo 25 "Bruselas I bis"): es lo que se conoce como una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional»[50]. El artículo 25 dicta que "si las partes, con independencia de su domicilio, han acordado que un órgano jurisdiccional o los órganos jurisdiccionales de un Estado miembro sean competentes para conocer de cualquier litigio que haya surgido o que pueda surgir con ocasión de una determinada relación jurídica, tal órgano jurisdiccional o tales órganos jurisdiccionales serán competentes".

2. Sumisión Tácita (artículo 26 "Bruselas I bis"). La siguiente conducta procesal de las partes significará que estamos ante una sumisión tácita: cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[51]; es decir, entra a discutir sobre el fondo del asunto.

---

[49] *Vid*. Albrecht, J. P. / Jotzo, F., *op. cit.* pp. 127-128. Aunque se ha entendido que los fueros del RGPD plantean conflictos con las competencias exclusivas del Reglamento "Bruselas I bis". *Cfr.* Brkan, M., "Data Protection and European Private International Law", *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, July 2015, p. 23.

[50] *Vid*. Ortega Giménez, A., "Imagen y circulación internacional de datos", *Revista boliviana de Derecho*, Núm. 15, Fundación Iuris Tantum, 2013, p. 138.

[51] *Vid*. Ortega Giménez, A., *op, cit.* p. 139.

3. Foro del domicilio del demandado (artículo 4 Reglamento "Bruselas I bis".) Este foro de competencia en un clásico de los instrumentos normativos de atribución de competencia. A falta de pacto expreso o tácito, el criterio atributivo de competencia es el del domicilio del demandado, que hace competentes a los tribunales del domicilio del demandado.

4. Foro especial en materia de obligaciones extracontractuales: el "lugar donde se hubiere producido o pudiere producirse el hecho dañoso". (artículo 7.3) del Reglamento "Bruselas I bis". Consiste en un foro especial regido por el principio de ubicuidad, que, en el caso de efectuar una acción por daños y perjuicios, el demandante tiene derecho a elegir entre los tribunales del lugar donde se produjo el hecho dañoso (ya sea donde se haya producido el hecho generador del daño o donde se padezca el daño) constituye la solución tradicional –y no siempre muy acertada– en esta materia[52]:

El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej. el Estado donde se recaban los datos), o el del lugar en que se verifica el resultado dañoso (p. ej. el Estado donde se acceden a los datos).

Como hemos observado, este artículo se caracteriza por una gran "dispersión competencial" que ataca directamente a la protección del titular del derecho a la protección de datos. A este artículo contribuyó a esclarecer la competencia judicial relacionada con litigios derivados de ilícitos contra los derechos de la personalidad la STJUE *eDate Advertising,* derivada de la doctrina instaurada por la STJCE *Fiona Shevill*[53], que interpretaba el antiguo artículo 5.3 del Reglamento Bruselas I. La STJCE *Fiona Shevill* permitía –y sigue permitiendo– a la víctima de la vulneración del derecho a la intimidad por la difamación de datos personales publicados y accesibles en varios Estados miembros ejercer una acción resarcitoria contra el promotor de la acción que causa el hecho dañoso ante los tribunales del domicilio de tal persona para reclamar una indemnización íntegra, o bien demandar ante los tribunales de cada Estado miembro el que la publicación sea difundida, y en el que la víctima alegue haber sufrido un ataque contra su reputación. La STJUE *eDate Advertising* viene a concretar y reducir esta "dispersión competencial" permitiendo que el afectado que alegue un daño o perjuicio en un Estado miembro exija una indemnización integral por todo el daño sufrido ante los

[52] *Vid. op. cit.* p. 142.

[53] STJCE de 7 de marzo de 1995, Asunto C-68/03, *Ixora Trading Inc; Chequepoint SARL, Chequepoint International Ld. C Press Alliance SA* ECLI:EU:C:1995:61.

tribunales del Estado promotor de la acción y el Estado donde la víctima tenga su centro de intereses.

3.1.2. Ley aplicable

La primacía de la legislación de protección de datos se manifiesta en una limitada autonomía de la ley aplicable en una cláusula contractual, la cual siempre deberá atenerse a los criterios del RGPD en los casos de obligaciones contractuales, cuyas cláusulas pueden estar sujetas a las leyes de otro Estado según el Reglamento (CE) 594/2008 "Roma I"[54]. Podemos tomar como ejemplo la STJUE *Amazon EU Sàrl,* la cual determinó como abusivas cláusulas sobre ley aplicable cuando no se cumplían los requisitos del artículo 6.2 del Reglamento "Roma I"[55].

Pero hay supuestos de responsabilidad extracontractual –como es el caso de las transferencias internacionales de datos– que plantean importantes problemas en cuanto al Derecho aplicable. La ley que resuelve esta controversia es el Reglamento (CE) 864/2007 "Roma II"[56].

El Reglamento "Roma II" es un texto legal con carácter universal[57]; es decir, la ley designada por el Reglamento se aplica aunque no sea de un Estado miembro, la cual permite una mayor y mejor unificación del mercado anterior[58]; pero que excluye de su aplicación en su artículo 1.2.g) "las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación", por tanto, las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia del tratamiento de sus datos personales por un responsable o encargado están excluidas de la norma, exclusión muy criticada por la doctrina[59].

---

54 DOCE L 177/6, de 4 de julio de 2008.

55 En este sentido se pronuncia la STJUE *Amazon EU Sàrl* (párrafo 71).

56 DOCE L 199/40, de 31 de julio de 2007.

57 Artículo 3.

58 *Vid*. Ortega Giménez, A., *Transferencias internacionales de datos…, op, cit.,* p. 138.

59 *Vid*. Dickinson, A.,*The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008, p. 240; Sancho Villa, D., *Negocios internacionales de tratamiento de datos personales*, Ed. Civitas, Navarra, España, 2010, pp. 97-98; Ortega Giménez, A., "La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español", *Diario La Ley,* Núm. 8661, 2015, p. 8; Brkan, M., "Data Protection and European Private International Law", *op. cit.* pp. 27-28; y De Miguel Asensio, P. A., "Competencia…", *op. cit.,* pp. 41-42.

La consecuencia de la no regulación conlleva a la aplicación de normas autónomas como el artículo 10.9 del Código Civil, que hace que apliquemos la ley del lugar donde se ha cometido el hecho (*lex loci delicti commissi*)[60]. La *lex loci delicti commissi* es una conexión de carácter territorial cuya aplicación en los supuestos de ilícitos en los elementos constitutivos (acto y resultado) se encontraban en un mismo Estado[61]. Pero en este ámbito, la precisión del lugar en el que se produce el daño puede resultar controvertida en situaciones en las que las consecuencias lesivas del hecho dañoso no son de carácter material, y esta norma no precisa cuál es el lugar del daño en las situaciones en las que el hecho causal y el resultado lesivo se producen en distintos países[62].

El artículo 10.9 del CC nos otorga dos opciones para determinar la ley aplicable: 1) la aplicación de la *lex loci actus* (Ley del Estado en el que se produce el hecho del que deriva la responsabilidad); o 2) la aplicación de la *lex loci damni* (aplicación de la ley del lugar donde se materializa el daño para las víctimas). Esta doble interpretación –o ambigüedad– puede ser solventada mediante la separación de ambos criterios en la Ley, como hacen algunos países de nuestro entorno.

En la primera opción (*lex loci actus*), el mayor problema que encontramos es determinar cuál es el Estado en el que se ha realizado el hecho dañoso, puesto que el hecho ilícito deriva de una cadena de ilícitos que se suelen desarrollar en otros Estados, el cual debemos verificar el Estado donde refleja sus efectos lesivos; esto es, el tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño[63][64]. Entonces, para poder aplicar la legislación española**,** a) el responsable del fichero tuviera su domicilio fuera de la UE y, b) el tratamiento de datos se hubiera realizado en España.

---

60 "Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven".

61 *Vid*. Vinaixa Miquel, M., *La responsabilidad civil por contaminación transfronteriza derivada de residuos*, Universidade de Santiago de Compostela, Santiago de Compostela, España, 2006, p. 147.

62 De Miguel Asensio, P. A., *Derecho privado de internet,* 4ª ed., Ed. Civitas, Madrid, España, 2011, p. 201.

63 *Vid*. Ortega Giménez, A., *Transferencias internacionales de datos…, op, cit.,* p. 143.

64 Respecto al caso BGH NJW 2011, 2059 comentado anteriormente, el *Bundesgerichtshof* señaló explícitamente que la aceptación de la jurisdicción también conduciría a la aplicación del Derecho alemán (artículo 40 (1) del EGBGB).

En cuanto a la segunda opción (*lex loci damni*), y en concreto en los supuestos de mero acceso, debe rechazarse que cualquier lugar de recepción de los contenidos o la información transmitidos por Internet sea por esa simple circunstancia lugar del daño debido a 1) que muchas veces ese acto no genera un daño "real" al titular, y 2) la aplicación de la ley de cada uno de los múltiples lugares de manifestación del daño puede conducir a una excesiva fragmentación normativa[65]. Es por ello que se afirma que el lugar donde se manifiesta la consecuencia directa para la víctima, se corresponde con el lugar de su residencia habitual como el centro de las relaciones sociales, personales y económicas susceptibles de verse afectadas por un atentado contra la intimidad u otros derechos de la personalidad; como ya comentamos a raíz de la STJUE *eDate Advertising*, no solo se materializa el perjuicio en el Estado de residencia habitual, también en aquel Estado en el que existan un vínculo estrecho con ese otro Estado.

A todo esto, debemos resaltar las precisiones del RGPD; ya que la tendencia que genera el artículo 79.2 del RGPD invita a aplicar "la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado"[66]. Su postura se basa en el objetivo que tiene la norma de proteger al afectado, el cual una de las maneras de plasmarlo es la aplicación de un Derecho que sea familiar al afectado que se correspondan con el del Estado de la residencia habitual (o del centro de intereses del afectado); y que entendemos que esta deba ser la opción que mejor puede llegar a proteger los intereses del afectado en función del principio de *favor laesi*[67]. Y en la práctica podemos prever que el demandante inicie las acciones en o bien el Estado de la residencia habitual, o bien en el centro de intereses del afectado, se aplicará la ley del Estado que asumió la competencia (*lex fori*).

3.2. Protección del algoritmo y las bases de datos

3.2.1. Competencia judicial

Como hemos dicho, la protección del algoritmo debe ventilarse mediante la protección del secreto empresarial derivada de la Directiva 2016/943 y la

---

65 *Vid*. De Miguel Asensio, P. A., *Derecho privado de internet*, *op. cit*., p. 203.

66 *Vid*. De Miguel Asensio, P. A., "Competencia…", *op. cit.* p. 42.

67 *Vid*. Ortega Giménez, A., "Propuestas ante un futuro incierto para la protección en la Unión Europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto vs. Armonización a través de unos principios comunes?", *Unión Europea Aranzadi*, Núm. 10, 2015, p. 6.

Ley de Competencia desleal. Los ilícitos sufridos por la violación de un secreto empresarial pueden ventilarse mediante un incumplimiento contractual.

Desde la perspectiva de una infracción extracontractual, cabe remitirse, en primer lugar, al Reglamento (UE) 1215/2012 y la legislación autónoma, el cual se observan dos posibles foros concurrentes:

El foro del domicilio del demandado del artículo 4.1: En este sentido, supone la norma general del Reglamento, donde no se tiene en cuenta dónde se ha llevado la actividad ilícita. Este foro opera cuando el demandado se encuentre en la UE.

1. Foro para supuestos de responsabilidad extracontractual del artículo 7.2. La existencia de este foro exige identificar previamente la localización de los actos de competencia desleal. Esto puede ligarse al lugar donde se realiza un tratamiento de datos sobre la base de dicho algoritmo o base de datos, o los tribunales del Estado donde se comercializan productos sobre la base de la explotación de dichos elementos; por lo tanto, será necesario identificar qué establecimientos realizan el tratamiento, y en qué Estados se está explotando el producto, por lo que puede darse el caso de poder ser competentes varios tribunales. Por lo tanto, el criterio de *forum delicti commissi* debe entenderse como tanto por lugar de realización de hecho generador del daño, como por lugar de producción del resultado[68]. Esta concurrencia de foros provoca una multiplicación de foros competentes y asimismo generar riesgos de *forum shopping*[69].

Es posible que los efectos dañosos puedan darse a futuro, el mero hecho de poseer los secretos para su explotación supone un acto ilícito que debe ser indemnizable, y por los cuales se pueden solicitar medidas cautelares en virtud del artículo 35[70] ante dicho juez competente.

Desde la perspectiva contractual, los casos de vulneración del *know-how* son poco habituales, pero en caso de que exista una relación jurídica preexistente, será de aplicación los foros de responsabilidad contractual. Pongamos el supuesto de que se encarga el tratamiento de los datos a otra empresa, la cual lleva aparejada la tecnología para realizar dicho tratamiento

---

68 STJUE, de 30 de noviembre de 1976, *Bier contra Mines de Potasse d'Alsace*.

69 *Vid*. Cornut, E., *Forum shopping et abus du choix du for en droit international privé*, *Journal du droit international privé*, Núm. 1, Enero 2007.

70 *Vid*. Font Segura, A., *La protección del secreto empresarial*, Colección Estudios internacionales, Eurolex D.L., Madrid, España, 1999, pp. 170-171.

para, posteriormente, devolver las conclusiones del análisis al responsable; pero que dicho encargado los utiliza por cuenta propia. En este sentido, los tribunales competentes serán los del Estado donde deba cumplirse la obligación. En caso de que existan varios establecimientos de la parte demandada, que puede interpretarse como "cualquier lugar donde se lleve dicho tratamiento de los datos, ya sea mediante la explotación del algoritmo o de la base de datos".

3.2.2. Ley aplicable

Cabe diferenciar entre responsabilidad extracontractual y responsabilidad derivada de un incumplimiento contractual.

Para el primer caso, cabe aplicar el Reglamento (CE) 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales, en concreto su artículo 6. Como observamos, este artículo contempla una regla especial en caso de daños derivados de actos de competencia desleal que afecten a los consumidores, y otra general cuando afecte a competidores en particular, que activará la aplicación del artículo 4, que permitirá la aplicación de la ley del Estado donde se produce el daño, sin tener en cuenta dónde se hayan generado. Aun así, existe el límite de la aplicación de las leyes de policía del artículo 16, cuyas leyes serán de aplicación imperativa. En el caso español, cualquier acto de competencia desleal que tenga efectos en el mercado español, será de aplicación la Ley de Competencia Desleal, y cuya aplicación ya se ha resuelto en los tribunales[71].

Respecto a la ley aplicable en las relaciones contractuales, cabe remitirse al propio Reglamento "Roma I" y las estipulaciones propias del contrato que acuerden las partes.

4. Reflexiones finales

PRIMERA.- ¡En *Big Data* no todo es protección de datos! En un mundo globalizado como el actual, las consecuencias jurídicas del *Big Data* van más allá de los datos personales y su incidencia alcanza a los secretos industriales. Esta tecnología se caracteriza por la afección a los datos personales, pero se obvian los fuertes elementos empresariales que la sustentan. Se ha observado que dos de los elementos nucleares del *Big Data*, como son el algoritmo y las

[71] STS (Sala de lo Civil, Sección 1ª), de 29 de octubre de 2014, Núm. 570/2014.

bases de datos no pueden protegerse por las herramientas clásicas que aporta el Derecho, como son la propiedad intelectual o la propiedad industrial, por lo que es necesario recurrir a la normativa de protección del *know-how* a través de la Ley de Competencia Desleal (que se encuentra en proceso de adaptación a la Directiva 2016/943).

SEGUNDA.- *Big Data* y que ¡Viva el Derecho Internacional Privado! En un mundo globalizado, es fácil la irrupción de litigios jurídicos a escala internacional, y cuyas previsiones desde el Derecho Internacional Privado se encuentran cubiertas por la unificación que presentan las normas europeas.

En definitiva, a nuevas realidades (*Big Data*) nuevos problemas (vulneración del derecho a la protección de datos de carácter personal, explotación de la base de datos mediante el uso del algoritmo, etc.), reinterpretación de las clásicas soluciones de Derecho Internacional Privado (así, p. ej., para poder determinar el lugar donde se produce el daño, será necesario acudir al concepto de establecimiento del responsable donde se realiza un tratamiento de datos personales. Así, respecto a la explotación de la base de datos mediante el uso del algoritmo para determinar la competencia judicial internacional que, en caso de la existencia de varios establecimientos, se puede dar el caso de la existencia del *forum shopping*, poniendo en una situación de ventaja al demandante sobre el demandado, al poder acudir el afectado ante los tribunales del Estado promotor de la acción y el Estado donde la víctima tenga su centro de intereses, que resolverá aplicando su ley –*lex fori*–).

5. Bibliografía

Brkan, M., "Data Protection and European Private International Law", *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, Julio, 2015.

Buyya, R. / Calheiros, R. / Vahid Dastjerdi, A., *Big Data: Principles and Paradigms*, Elsevier, Amsterdam, Países Bajos, 2016.

Conesa Caralt, J. (Coord.) / Curto Díaz, J., *Introducción al Business Intelligence*, Ed. UOC, Barcelona, España, 2012.

Cornut, E., *Forum shopping et abus du choix du for en droit international privé*, *Journal du droit international privé*, Núm. 1, Enero 2007.

Davara Rodríguez, M. A., "Big Data", *El Consultor de los Ayuntamientos,* Núm. 15, Ed. Wolters Kluwer, Madrid, España, 2013.

De Miguel Asensio, P. A., *Derecho privado de internet,* 4ª Ed., Ed. Civitas, Madrid, España, 2011.

Deloitte, "Big Data, Big Brother? Striking the right balance with privacy", 2015.

Díaz Granados Ordoñez, G. F., "La comercialización del *Big data and commercial* law", *Univ. Estud. Bogotá*, Núm. 14, julio-diciembre 2016.

Dickinson, A., *The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008.

Elias, H., "El desafío de *Big Data*: Cómo desarrollar una estrategia ganadora", CIO, Julio 2012.

European Commission, "Worldwide Big Data Technology and Services 2012-2015 Forecast", *IDC Report*, Marzo, 2012.

Font Segura, A., *La protección del secreto empresarial*, Colección Estudios internacionales, Eurolex D.L., Madrid, España, 1999.

Garriga Domínguez, A., *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, España.

González Royo, I., "La protección de los intangibles intelectuales e industriales en el contexto del Fintech", *Diario La Ley*, Núm. 8795, 2016.

González Royo, I. / Pina, C., "¿Cómo se protegen legalmente los algoritmos?", *Diario La Ley*, Núm. 8776, 2016.

Hua Tan, K. / Ji, G. / Peng Lim, C. / Tseng, M.-L., "Using big data to make better decisions in the digital economy", *International Journal of Production Research*, Núm. 17, Vol. 55, 2017.

Jain, V. K., *Big data and Hadoop*, Khanna Publishing, New Delhi, India, 2017.

Mayer-Schönberger, V. / Cukier, K., *Big Data. A Revolution That Will Transform How We Live*, Ed. Houghton Mifflin Harcourt, New York, Estados Unidos de América, 2013.

Orejudo Prieto de los Mozos, P., "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, Núm. 4, 2013.

Ortega Giménez, A., "Imagen y circulación internacional de datos", *Revista boliviana de Derecho*, Núm. 15, Fundación Iuris Tantum, 2013.

Ortega Giménez, A., "La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español", *Diario La Ley,* Núm. 8661, 2015.

Ortega Giménez, A., "Propuestas ante un futuro incierto para la protección en la Unión Europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto vs. Armonización a través de unos principios comunes?", *Unión Europea Aranzadi*, Núm. 10, 2015.

Puyol Montero, J., *Aproximación jurídica y económica al Big Data*, Ed. Tirant lo Blanch, Valencia, España, 2016.

Sánchez Bravo, A. (Ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez*, Ed. Punto Rojo Libros, Sevilla, España, 2014.

Sancho Villa, D., *Negocios internacionales de tratamiento de datos personales*, Ed. Civitas, Navarra, España, 2010.

Savirimuthu, J., "Do algorithms dream of 'data' without bodies?", *International Review of Law, Computers & Technology*, Núm. 2, Vol. 31, 2017.

Soares, S., "Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today", *Big Data Governance. An Emerging Imperative*, Ed. MC Press, Boise (Idaho), Estados Unidos de América, 2012.

Starmans. J. C. M. R., "The Advent of Data Science: Some Considerations on the Unreasonable Effectiveness of Data", *Handbook of Big Data*, Bühlmann, P. / Drineas, P. / Kane, M. / Van der laan, M., CRC Press, Boca Raton (Florida), Estados Unidos de América, 2016.

Tascón, M. / Coullaut, A., *Big Data y el Internet de las Cosas. Qué hay detrás y cómo nos va a cambiar*, Ed. Catarata, Madrid, España, 2016.

Vedder, A., "Accountability for the use of algorithms in a big data environment", *International Review of Law, Computers & Technology*, Núm. 2, Vol. 31, 2017.

Vinaixa Miquel, M., *La responsabilidad civil por contaminación transfronteriza derivada de residuos*, Universidade de Santiago de Compostela, Santiago de Compostela, España, 2006.

Vivas-Tesón, I., "La tutela `sui generis´ de las bases de datos", *Revista de Derecho Patrimonial*, Núm. 21, 2008.

Zikopoulos, P.C., *Harness the power of big data, the IBM Big data platform*, Ed. McGraw-Hill, New York, Estados Unidos de América, 2013.

La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018*

Legitimation for the processing of special categories of data for research purposes within the framework of Regulation (EU) 2016/679 and Fundamental Law 3/2018

Miriam Méndez García
Hospital Clínic de Barcelona (Barcelona, España)

Iciar Alfonso Farnós
Comité de Ética de la Investigación con medicamentos de Euskadi (Vitoria, España)

DOI: 10.14679/1137

Sumario / Summary: 1. Introducción. 2. Antecedentes normativos. 3. Cambio legislativo y condiciones que deben concurrir para tratar datos de salud en base al Reglamento (UE) 2016/679 y la LOPD-GDD. 4. Reutilización de datos de salud. Condiciones y límites. 5. Seudonimización. ¿medida de seguridad o habilitación

* Artículo recibido el 19 de febrero de 2019 y aceptado para su publicación el 6 de junio de 2019.
Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos –*Big Data*–. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

legal para tratar los datos de salud con finalidades de investigación biomédica? 6. Estudios en materia de salud pública. 7. Requisitos adicionales al uso de datos con finalidades de investigación previstos en el artículo 89 del Reglamento (UE) 2016/679. 8. Discusión. 9. Conclusiones. 10. Bibliografía.

Resumen / Abstract: La entrada en vigor del Reglamento (UE) 2016/679 del Parlamento y el Consejo Europeo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (en adelante Reglamento (UE) 2016/679), y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD-GDD), supone un impacto directo en las condiciones de uso de datos de salud o datos genéticos para investigación biomédica. A través del Reglamento (UE) 2016/679, y en especial de la Disposición Adicional decimoséptima de la LOPD-GDD, se regulan las condiciones de uso de datos de salud y genéticos con finalidades de investigación, introduciendo novedades en cuanto a su uso y ofreciendo nuevas bases de legitimación para su uso, siendo necesario analizar la incidencia práctica que van a tener.

The entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (here in after Regulation (EU) 2016/679), and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (in forward LOPD-GDD), implies a direct impact on the conditions of the use of health data or genetic data for biomedical research.

The Regulation (EU) 2016/679, and especially the additional seventeenth provision of LOPD-GDD, establish the conditions for the use of health and genetic data for research purposes and introducing and offering new bases of legitimacy for their use. It is necessary to analyze the practical implications that they are going to have.

Palabras clave / Keywords:

Categorías especiales de datos / Consentimiento informado / Investigación biomédica / Seudonimización.

Special categories of data / Informed consent / Biomedical research / Pseudonymization.

1. Introducción

La publicación del Reglamento (UE) 2016/679 del Parlamento y el Consejo Europeo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (en adelante Reglamento (UE) 2016/679), y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD-GDD), han introducido un nuevo marco regulatorio en la investigación con datos en España.

Hasta la fecha la normativa que regulaba la investigación con datos eran la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) respecto al tratamiento de datos de carácter personal y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LAP), como norma que regula la información y documentación clínica. Uno de los problemas principales que se planteaba en la investigación observacional era la obligación, exigida por la LOPD, de solicitar el consentimiento del afectado para tratar los datos con fines de investigación.

El Reglamento General de Protección de Datos (UE) 2016/679 ha incluido importantes novedades en relación a la investigación sanitaria con datos personales. El Reglamento (UE) 2016/679, y en especial la Disposición Adicional decimoséptima de la LOPD-GDD, regulan las condiciones de uso de datos de salud y genéticos con finalidades de investigación, introduciendo novedades en cuanto a su tratamiento y ofreciendo nuevas bases de legitimación para su uso. El objetivo de este trabajo es analizar la incidencia práctica de estas novedades en las condiciones de uso de datos de salud o datos genéticos para realizar investigación biomédica.

2. Antecedentes normativos

Antes de la entrada en vigor del Reglamento (UE) 2016/679 y de la LOPD-GDD, 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 a la libre circulación de estos datos, y la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos, establecían que el uso de datos de salud (denominados especialmente sensibles) sólo podía basarse en tres supuestos, el consentimiento expreso del titular de los mismos, la anonimización o la autorización para su uso mediante una norma con rango legal.

Si atendemos al marco legal aplicable a la investigación con muestras biológicas, antes de la entrada en vigor del Reglamento (UE) 2016/679, y la LOPD-GDD, ya podíamos encontrar una excepción que permitía utilizar datos de salud para investigación en el caso de la información asociada al uso de muestras biológicas. Este uso era posible cuando se daban los requisitos necesarios para que un Comité de Ética de la Investigación (CEI) autorizará su uso sin consentimiento, siempre y cuando concurrieran los requisitos

establecidos por la Ley 14/2007, de 3 de julio, de Investigación Biomédica (en adelante LIB), y el Real Decreto 1716/2011, de 18 de noviembre, que establece los requisitos básicos de autorización y funcionamiento de los Biobancos con finalidades de investigación biomédica y de tratamiento de las muestras biológicas de origen humano, y que regula el funcionamiento y organización del Registro Nacional de Biobancos para la Investigación Biomédica.

Así mismo existían ejemplos prácticos de explotación de datos de forma masiva con finalidades de investigación, como por ejemplo el Programa de analítica de datos para la investigación y la innovación en salud (en adelante "PADRIS") en Catalunya[1], que permitía la reutilización para investigación de datos procedentes de los ficheros creados con finalidades de asistencia, gestión y control sanitario, titularidad del ente gestor de la sanidad en Catalunya. En este sentido, el programa PADRIS establece una serie de cautelas para garantizar los derechos de los titulares de los datos, basados en:

- El proceso de anonimización de los datos.

- El acceso a los datos limitado a investigadores del entorno investigador y asistencial público.

- La exigencia, de forma previa al acceso a los datos, de un acuerdo firmado que regule el uso que se puede dar a los datos, y en el que justifique el interés científico del proyecto.

- La posibilidad de los titulares de los datos de oponerse a que sus datos asistenciales se incorporen al programa PADRIS.

Más allá de estos supuestos, en la práctica diaria de los investigadores se acababa constatando que sólo era posible utilizar los datos para investigar o bien anonimizándolos, o bien solicitando un consentimiento expreso. La normativa del sector sanitario no permitía encontrar una excepción que autorizara el uso de datos para investigación prescindiendo del consentimiento del sujeto titular de los datos para proyectos concretos.

Cuando la normativa hablaba de consentimiento expreso se interpretaba como circunscrito a un proyecto de investigación determinado, ya que las Autoridades de Protección de Datos interpretaban que no era posible obtener un consentimiento a priori sin conocer el proyecto concreto de investigación,

[1] Página web del proyecto PADRIS: http://aquas.gencat.cat/ca/projectes/analitica_dades/

no aceptando un consentimiento para utilizar datos, por ejemplo, para determinadas enfermedades de la misma especialidad.

Así mismo, el concepto de anonimización se entendía como la eliminación de cualquier dato que permitiera identificar al sujeto a quien pertenecían los datos de forma irreversible, de forma que una vez se anonimizaba no se podía reidentificar al sujeto de nuevo.

En este sentido, los investigadores, más allá de los proyectos de investigación donde hay contacto directo con los pacientes, como por ejemplo los ensayos clínicos, cuando estaban en el ámbito de estudios retrospectivos, dónde contactar con el paciente requiere un esfuerzo no razonable, se enfrentaban a serias dificultades para legitimar el uso de estos datos mediante el consentimiento del paciente. Si bien existía la opción de anonimizar, esto no siempre era posible porque restaba valor a la investigación, ya que con frecuencia es necesario recabar nuevos datos del sujeto.

Esta situación se agrava a medida que van entrando en juego las tecnologías que permiten la explotación masiva de datos, en un entorno donde la anonimización total ya no se puede garantizar, las tendencias de la comunidad científica van hacia compartir recursos (open data) y prolifera la explotación masiva de datos con finalidades de investigación. Por consiguiente, el esquema tradicional del consentimiento, como se había entendido hasta el momento, circunscrito a un proyecto definido, no servía, siendo necesario encontrar otras fórmulas.

3. Cambio legislativo y condiciones que deben concurrir para tratar datos de salud en base al Reglamento (UE) 2016/679 y la LOPD-GDD

Con la entrada en vigor del Reglamento (UE) 2016/679, y en especial de la Disposición Adicional 17 de la LOPD-GDD, se introducen nuevos supuestos y, conjuntamente con la interpretación de la normativa sectorial, se abren nuevas perspectivas para el uso de datos de salud y de tipo genético para investigación biomédica, algunas con aplicación directa en el ámbito de la explotación masiva de datos.

En este ejercicio interpretativo debemos tener en cuenta las guías que nos da la normativa sobre investigación, así como las normas del sector salud, como LAP, la LIB, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del

Sistema Nacional de Salud o la Ley 33/2011, de 4 octubre, General de Salud Pública, así como la regulación relativa a ensayos clínicos y a otro tipo de proyectos de investigación.

Son reseñables dos dictámenes emitidos recientes por la Autoridad Catalana de Protección de Datos (en adelante "APDCAT"), desarrollados a continuación, en los que se analiza el régimen establecido por la Disposición Adicional 17 de la LOPD-GDD, para el tratamiento de datos de salud en el marco de la investigación, estos dictámenes son el 15/2019, dónde se analiza, como se explica a continuación, el tratamiento de datos seudonimizados con finalidades de investigación, y el Dictamen 18/2019, que analiza otros aspectos de la Disposición Adicional 17 de la LOPD-GDD.

En la misma línea de los Dictámenes de la APDCAT, también debemos examinar el Dictamen 3/2019, sobre "Preguntas y Respuestas sobre la interrelación entre la regulación de ensayos clínicos y el Reglamento (UE) 2016/679 (RGPD)" de 23 de enero de 2019, del Comité Europeo de Protección de Datos (EDPB)[2].

En cuanto a la normativa de protección de datos debemos acudir a los artículos 6, 9, 13 y 89 del Reglamento (UE) 2016/679, al artículo 9, 11 y a la Disposición Adicional 17 y Disposición Transitoria 6 de la LOPD-GDD, para ver en qué condiciones se establecen las obligaciones de información y consentimiento para el tratamiento de las categorías especiales de datos, dentro de las que se incluyen los datos de salud y genéticos.

Así mismo, la Disposición Adicional 17 de la LOPD-GDD, prevé otras formas de legitimar el tratamiento de datos en el ámbito de la salud más allá del consentimiento del titular de los datos. En este sentido se pronuncia la APDCAT en el Dictamen 15/2019 y 18/2019, que específicamente realiza un estudio de los supuestos en los que la base legitimadora del tratamiento de los datos con finalidades de investigación no es el consentimiento.

---

[2] El EDPB afirma que debe diferenciarse las actividades de tratamiento relacionadas con la fiabilidad y seguridad derivadas directamente de las obligaciones legales del responsable, enmarcadas en la base legal del Artículo 6 (1) (c) en relación con el Artículo 9 (1) (i) de RGPD. Para el resto de actividades de tratamiento de datos, relacionadas con actividades de investigación, se contemplan tres bases legales alternativas, dependiendo de las circunstancias de un ensayo clínico específico: tareas realizadas en el interés público conforme al Artículo 6 (1) (e) en relación con el Artículo 9 (2), (i) o (j) del RGPD; los intereses legítimos del responsable en virtud del Artículo 6 (1) (f) en relación con el Artículo 9 (2) (j) del RGPD y en circunstancias específicas, cuando se cumplen todas las condiciones, el consentimiento explícito del interesado en virtud del Artículo 6 (1) (a) y 9 (2) (a) del RGPD.

Los requisitos relativos a la información que debe recibir el titular de los datos y la forma en que se debe proporcionar están definidos en el artículo 13 del Reglamento (UE) 2016/679 y el artículo 11 de la LOPD-GDD. Estos artículos establecen los requerimientos y el contenido que debe tener la información que el responsable del tratamiento debe proporcionar a los titulares de los datos, de forma que se garantice que este conoce la identidad del responsable, las condiciones en que se tratarán sus datos, cuáles son sus derechos y la forma de ejercerlos.

El Reglamento (UE) 2016/679, más allá de la enumeración formal del contenido del deber de información, en su artículo 13.3, establece:

> "Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2[3]".

Así pues, resulta interesante la mención a *la posibilidad de utilizar datos para finalidades distintas a las indicadas en el consentimiento.* Esta previsión permite interpretar que el legislador europeo admite la posibilidad de abrir la puerta al uso de los datos más allá del consentimiento del titular de los datos.

Precisamente, tal y como veremos más adelante, esta posibilidad se ha desarrollado por el legislador español a través de la Disposición Adicional 17.2.C. y la Disposición Transitoria 6 de la LOPD-GDD.

El artículo 6 del Reglamento (UE) 2016/679 establece las bases que legitiman el tratamiento de datos personales, y el artículo 9 establece las condiciones de tratamiento de las categorías especiales de datos, dentro de los que se encuentran los datos de salud y los datos genéticos.

El artículo 6.1.a, establece:

> *"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio* ***su consentimiento*** *para el tratamiento de sus datos personales para uno o varios fines específicos;…".*

Y el artículo 9, en relación al tratamiento de las categorías especiales de datos personales, establece:

[3] El apartado 2 del art. 13 hace referencia a la Información que deberá facilitarse para garantizar un tratamiento de datos leal y transparente.

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;"

Así pues, de la interpretación conjunta de los artículos 6 y 9 del reglamento, podemos concluir que la norma general establece que para tratar categorías especiales de datos debe concurrir el consentimiento expreso del titular de los mismos. En el mismo sentido se pronuncia el artículo 9 de la LOPD-GDD que remite el tratamiento de las categorías especiales de datos a lo establecido en el artículo 9.2 del Reglamento (UE) 2016/679.

En este punto debemos ahondar cómo entendemos el concepto de consentimiento expreso, ¿debe equipararse a consentimiento por proyecto?

Tradicionalmente siempre se ha solicitado el consentimiento por proyecto de investigación, y las Agencias o Autoridades de Protección de Datos no admitían el *consentimiento abierto para proyectos relacionados con una misma enfermedad o área de investigación* (tal y como admite la Ley de Investigación Biomédica para las colecciones de muestras o para muestras almacenadas en un biobanco), por considerar que no responde a las características de un consentimiento explícito.

En este sentido se debe destacar *el considerando 33* del Reglamento (UE) 2016/697, que admite la posibilidad de los *consentimientos por área de investigación*. Concretamente establece:

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

En esta línea se ha manifestado la Agencia Española de Protección de Datos, en el *Informe 073667/2018*[4], indicando que es posible admitir el consentimiento por áreas de investigación, atendiendo precisamente a lo establecido en el considerando 33 del Reglamento (UE) 2016/679.

La entrada en vigor de la LOPD-GDD ha confirmado esta interpretación y ha establecido a través de su Disposición Adicional *decimoséptima:*

> *"2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: a) El interesado o, en su caso, su representante legal podrá otorgar el* ***consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora".***

Así pues, podemos afirmar que se admite el consentimiento para el uso de *los datos de salud y los datos genéticos en el ámbito de la investigación mediante la obtención de un consentimiento con fines de investigación en salud que abarque categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.*

Así mismo, en relación al tratamiento de los datos genéticos, debemos tener en cuenta también las salvaguardas establecidas por la LIB y la Declaración Internacional sobre los Datos Genéticos Humanos de 16 de octubre de 2003. Concretamente estos dos textos inciden en la importancia del derecho de los sujetos, origen del dato genético, de conocer y no conocer los resultados de la investigación. A pesar de no estar previsto en la normativa de protección de datos es importante tener en cuenta el cumplimiento de estos derechos al tratar datos de tipo genético.

Esta previsión contemplada en la LOPD-GDD abre la puerta a pedir los consentimientos más allá de un proyecto de investigación, haciendo un símil con la legislación que regula el uso de muestras humanas para investigación, y que permite el consentimiento por líneas de investigación.

Esta fórmula de *consentimiento amplio* permitirá solucionar algunos de los problemas con los que se encontraban los investigadores, abriendo la puerta a la creación de bases de datos/registros por áreas de investigación.

---

[4] Disponible en: https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

En este sentido, será recomendable que los centros sanitarios y de investigación focalicen sus esfuerzos en elaborar unos modelos de consentimiento informado que contengan todos los puntos legalmente exigibles y en los que se prevea la posibilidad de utilizar los datos de un estudio para otros proyectos enmarcados en la misma área de investigación, estableciendo los cauces para garantizar el deber de información a los interesados.

De la misma forma que, de conformidad con la Ley de Investigación Biomédica, es factible la creación de colecciones de muestras, se podrán crear "colecciones" de datos para ser usados en una determinada área de investigación. Ante esta opción podemos plantearnos las siguientes cuestiones:

- ¿Quién puede acceder a estas "bases de datos" para hacer investigación, cualquier investigador del centro o sólo el investigador que solicitó el consentimiento?

  Aquí parece lógico contestar que cualquier investigador del centro de investigación podría acceder a estos datos, siempre teniendo en cuenta la limitación de la propia área de investigación y los derechos de acceso a las historias clínicas.

- ¿Qué sucede cuando los investigadores realizan colaboraciones con otras instituciones, actividad muy frecuente en el ámbito de la investigación biomédica? ¿Podríamos admitir que el investigador compartiera datos con su grupo de investigación aunque fueran de otras entidades?

La legislación no se pronuncia en este punto, pero podríamos admitir un consentimiento por línea de investigación dónde se solicitara el consentimiento en este sentido, añadiendo unas cautelas adicionales como la seudonimización de los datos compartidos, las medidas adoptadas para garantizar el suministro de información a los interesados y la firma de acuerdos de cesión de datos, en el marco del proyecto, entre los diferentes colaboradores.

Así mismo, también debemos considerar si nos encontramos ante colaboraciones con intereses comerciales o no, ya que debería ser un factor a tener en cuenta para admitir o no que se compartan datos (seudonimizados) con otras instituciones.

Así pues, en relación a la excepción establecida en la Disposición Adicional 17.2.a podemos afirmar que permite crear bases de datos para

investigación por áreas o especialidades, pero plantea dudas acerca de la posibilidad de compartir estos datos.

El Dictamen 18/2019 de la APDCAT se ha pronunciado sobre la naturaleza del concepto de investigación prevista en la Disposición Adicional 17.2.a, entendiendo como aplicable a cualquier tipo de investigación, ya sea la prevista en el LIB, ensayos clínicos o estudios observacionales, pero no se ha pronunciado respeto la posibilidad de compartir esos datos.

4. Reutilización de datos de salud. Condiciones y límites

Además del consentimiento para el uso de datos de salud con finalidades de investigación biomédica, la LOPD-GDD establece, en su Disposición Adicional 17 y la disposición transitoria 6, la posibilidad de reutilizar los datos de salud.

En el caso de la Disposición transitoria 6 se establece:

> "Disposición transitoria sexta. Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.
> Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:
> a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.
> b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial".

La Disposición Transitoria 6 habilita para utilizar los datos que, *antes* de la entrada en vigor de la LOPD-GDD, se hayan recogido para llevar a cabo un estudio concreto y a posteriori se quieran utilizar para proyectos de investigación similares o en áreas de investigación relacionadas. Esta previsión no establece ningún requisito adicional para la reutilización de datos recogidos antes de la entrada en vigor de la LOPD-GDD, más allá que los estudios se encuentren dentro de la misma área de investigación o relacionada, ¿pero qué sucede con los datos recogidos después de la entrada en vigor de la LOPD-GDD?

La reutilización de datos de salud recogidos después de la entrada en vigor de la LOPD-GDD, para investigación científica se regula en el punto 2.c de la indicada Disposición Adicional 17 que establece:

> *"El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios…c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta,* ***se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial****. En tales casos, los responsables deberán* ***publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico,*** *y, en su caso, en la del promotor,* ***y notificar la existencia de esta información por medios electrónicos a los afectados****. Cuando éstos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato. Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación".*

Así pues, esta previsión abre la puerta a utilizar datos de salud para áreas de investigación relacionadas, siempre y cuando, como a continuación se desarrolla, se disponga de un dictamen favorable del CEI, y se publique la información relativa al uso de estos datos en la web del centro dónde se lleve a cabo el estudio, y si es el caso en la del promotor, así como que se notifique la existencia de este estudio a los titulares de los datos.

Esta excepción debe interpretarse a tenor de la modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante "Ley Transparencia") establecida por la LOPD-DGG. Concretamente la disposición final undécima de la LOPD-GDD modifica el artículo 15.1 de la Ley de Transparencia, que define en relación a la reutilización de datos *" (…) Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos (…), el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.".*

Esta modificación nos permite afirmar que la reutilización de datos de salud y datos genéticos queda sometido a un régimen específico, concreta-

mente el regulado por la Disposición Adicional 17.2 de la LOPD-DGG y no al general establecido por la Ley de Transparencia.

La redacción de esta Disposición Adicional 17.2.c genera algunas dudas, la primera de ellas, ¿cuáles son los datos que se pueden reutilizar, datos recogidos con fines asistenciales o datos procedentes de otros estudios?

Si bien parece lógico que la aplicación de este artículo se pudiera entender extensible a datos incluidos en las historias clínicas de los pacientes, la literalidad del artículo establece que "…***se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial…".*** ¿Debemos entender pues que estudio es equivalente a investigación o a estudio asistencial?

Así mismo en relación a los proyectos en los que se vayan a reutilizar datos, ¿quién los puede llevar a cabo? ¿El mismo investigador que llevó a cabo el estudio inicial, otros investigadores pero siempre dentro del marco del centro responsable del tratamiento? ¿Otras instituciones?

Desde un punto de vista de coherencia jurídica parecería lógico que la reutilización de datos se pudiera llevar a cabo únicamente dentro de la misma institución y circunscrito a datos procedentes de otros estudios de investigación, en analogía a lo establecido en el artículo 58 de la LIB.

En cuanto a quien tendrá acceso a estos datos podemos interpretar, al igual que el caso del consentimiento amplio, que será la institución en la que desarrolla su labor asistencial el investigador y, que, previa adopción de una serie de cautelas, se podrían compartir de forma seudonimizada con investigadores de otros centros que participen en un mismo proyecto de investigación.

A diferencia de lo que sucedía en el caso del uso de datos recogidos antes de la entrada en vigor de la LOPD-GDD, para los datos recogidos después de la entrada en vigor de esta norma, se exige que concurran unos requisitos adicionales. Estos requisitos adicionales son:

a. Aprobación del proyecto por un CEI. Este requisito es muy razonable, ya que todos los proyectos de investigación que impliquen el uso de datos personales deben aprobarse por un CEI, como ente garante de su buen uso.

b. La publicación y la comunicación al afectado de la información del estudio. Este requisito, si bien es necesario a efecto de dar cobertura

al derecho de información y transparencia que tienen los titulares de los datos, en la práctica resulta complejo saber cómo se hará efectivo, y el grado de cumplimiento real que tendrá. Las entidades que realicen investigación deberán articular los mecanismos necesarios para garantizar que los investigadores disponen de los recursos necesarios para poder dar cumplimiento a esta obligación. En este punto cobra especial relevancia el papel que debe llevar a cabo el Delegado de Protección Datos, asesorando a los investigadores en esta materia.

Debemos entender la reutilización de datos como la otra cara de la moneda del consentimiento por línea de investigación. Es decir, el consentimiento por línea de investigación permite obtener un consentimiento para usar datos en el marco de un área de investigación, y la reutilización de datos facilita la utilización de unos datos obtenidos con un consentimiento concreto, para otros proyectos de la misma área de investigación.

Esta interpretación, fundamentando que el uso de datos para investigación tiene su base en una interpretación amplia del ámbito del consentimiento, es muy importante para después determinar la aplicabilidad de determinados requisitos de la Disposición Adicional 17 de la LOPD-GDD.

En este sentido, la Agencia Española de Protección de Datos ha afirmado que "será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, como por ejemplo, la investigación oncológica, o incluso para ámbitos más extensos[5]".

Por otra parte, el uso de datos procedentes de las historias clínicas de los pacientes para investigación tendría otras vías de legitimación, como por ejemplo mediante la seudonimización, que se aborda a continuación.

5. Seudonimización. ¿medida de seguridad o habilitación legal para tratar los datos de salud con finalidades de investigación biomédica?

La primera pregunta a la que debemos dar respuesta es ¿que entendemos por seudonimización? El Reglamento (UE) 2016/679, en su artículo 4, define la seudonimización como:

[5] Agencia Española de Protección de Datos. Informe: 073667/2018, disponible en: https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

> "el tratamiento de datos personales de manera tal que ya no pueden atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y que esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Por consiguiente debemos tener en cuenta que cuando hablamos de dato seudonimizado, a efectos de la normativa de protección de datos, tiene la consideración de dato personal, a diferencia del dato anonimizado, por lo que le aplica la normativa de protección de datos, aunque con las excepciones que la propia normativa establece para el tratamiento de este tipo de datos. La APDCAT, en su informe 15/2019, también se pronuncia sobre este aspecto, y mantiene la consideración de dato personal al dato seudonimizado, y en consecuencia afirma que le son aplicables todos los principios y obligaciones de la normativa de protección de datos.

En este sentido, el artículo 89.1 del Reglamento (UE) 2016/679, establece en su punto 1:

> *"El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo".*

Podemos afirmar que este artículo abre la puerta a *tratar los datos con finalidades de investigación de forma seudonimizada siempre que la normativa interna de los estados lo permita.*

Si acudimos a la LOPD-GDD, en su Disposición Adicional 17, podemos establecer en qué condiciones concretas la *normativa española permite el uso de datos seudonimizados para investigación*. Concretamente establece:

> "2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá: 1º Una separación técnica y funcional

entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. 2° Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria". Y después en la letra g de la misma Disposición Adicional 17 añade " g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679".

De la lectura conjunta del artículo 89 del Reglamento (UE) 2016/679 y de la Disposición Adicional 17 2.d podemos hacer dos interpretaciones distintas. Una primera interpretación sería la de admitir que cuando la ley habla de habilitación legal es la propia Disposición Adicional 17.2.d quién la otorga y que cualquier tipo de dato de salud aplicándole medidas para seudonimizarlo se puede utilizar para investigación.

Una segunda interpretación consistiría en afirmar que podemos utilizar los datos de forma seudonimizada para finalidades de investigación siempre que exista una habilitación legal para ello, adicional a la previsión del artículo 17.2.d (como por ejemplo la LAP). Esta interpretación permitiría admitir la reutilización de cualquier dato contenido en las historias clínicas de pacientes, pero no permitiría el uso de bases de datos de salud que no formen parte de una historia clínica en base a esta excepción, aunque se podrían aplicar otras excepciones como la reutilización de datos.

Si acudimos al informe 15/2019 de la APDCAT descarta el consentimiento como única herramienta para el tratamiento de datos de salud en materia de investigación. El RGPD y la LOPD-GDD se posicionan en el sentido de admitir que se pueden tratar datos de categorías especiales con una base jurídica diferente del consentimiento, como la establecida por la Disposición Adicional 17, y la normativa sectorial de aplicación, como la LAP.

La segunda interpretación parece más ajustada a los principios de protección de datos, ya que abrir la puerta a utilizar cualquier dato para investigación previa seudonimización dejaría al titular de los datos en una situación de vulnerabilidad. De esta forma, podríamos entender que seudonimizando cualquier dato, ajeno a la actividad asistencial, y por tanto no amparado por la LAP, podría utilizarse para investigar, y esto podría permitir realizar estudios, por ejemplo por aseguradoras con los datos de sus asegurados, sin su consentimiento.

En el marco de los centros asistenciales, siempre será posible la seudonimización de datos para su uso para investigación (por supuesto con las cautelas, legalmente exigibles). Pero fuera del ámbito asistencial debe limitarse esta excepción para evitar una pérdida de garantías para el tratamiento de categorías especiales de datos

La Disposición Adicional 17.2.d concreta los requisitos mínimos que deben darse en la seudonimización de datos, y que a efectos prácticos supone que exista una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

Así mismo, los datos seudonimizados únicamente serán accesibles al equipo de investigación si:

- Existe un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

- Se adoptan medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

- El Comité de Ética emite el correspondiente dictamen favorable cuando se utilicen datos seudonimizados para investigación.

Tal y como hemos planteado anteriormente, la seudonimización debe ir acompañada de una habilitación legal para tratar el dato con finalidades de investigación, ya que si no supondría una carta en blanco que podría suponer un perjuicio al titular de los datos. Esta afirmación proviene de entender la Disposición Adicional 17.2.d de la LOPD-GDD como un desarrollo o concreción de lo establecido en el artículo 89 del Reglamento (UE) 2016/679.

Entendemos que los datos que se seudonimicen deben pertenecer al entorno asistencial y debe disponerse de una base legítima para su tratamiento.

En este sentido, cabe mencionar la LAP, que precisamente ha sido modificada a través de la disposición final novena de la LOPD-GDD, incluyendo este nuevo redactado:

> "16.3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición Adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso. Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos".

Este artículo entendemos que legitima el uso de datos pertenecientes a la historia clínica de un centro con finalidad de investigación siempre y cuando se seudonimicen en las condiciones establecidas por la propia Disposición Adicional 17. Así pues, la combinación de la seudonimización y el artículo 16.3 de la LAP permitiría utilizar los datos contenidos en la historia clínica de un centro, seudonimizarse y utilizarse con finalidades de investigación con los límites establecidos por esta normativa. En este caso, a diferencia de los dos casos anteriores (consentimiento por línea de investigación y reutilización de datos, donde la base legitimadora del tratamiento era el consentimiento), la base del tratamiento es la habilitación legal más la seudonimización de los datos.

6. Estudios en materia de salud pública

La Disposición Adicional 17.2.a contempla otra posibilidad en cuanto a la reutilización de los datos, en este caso en el ámbito de la salud pública, concretamente establece:

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

Esta excepción debe entenderse aplicable al concepto de salud pública que incorpora el RGPD, y que es el previsto en el Reglamento UE 1338/2008, así como la Ley 33/2011, de 4 de octubre, General de Salud Pública, y que refiere a varios ámbitos de la salud de la población, la investigación que resulta de interés público y que supone un beneficio para toda la población.

En este sentido cabe destacar la incidencia que esta previsión tendrá en áreas como las enfermedades de declaración obligatoria, donde los centros sanitarios están obligados a comunicar los casos de forma identificada a las autoridades competentes en la materia. A partir de esta excepción, este tipo de entidades podrán utilizar los datos que obtengan de todos los centros sanitarios con finalidades de investigación, si concurren los requisitos establecidos a tal efecto.

Esta excepción permite el uso de datos para investigaciones de salud pública cuando existan situaciones de excepcional relevancia y gravedad, sin necesidad de consentimiento, con el significado indicado en el segundo párrafo de este apartado 6.

7. Requisitos adicionales al uso de datos con finalidades de investigación previstos en el artículo 89 del reglamento (UE) 2016/679

Finalmente, la letra f de la Disposición Adicional 17 establece:

> f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:
> 1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Regla-

mento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.
2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.
3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.
4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

¿Esta previsión debe interpretarse de forma cumulativa al resto de requisitos a todos los casos previstos en la Disposición Adicional 17.2?

Para dar respuesta a esta pregunta tenemos que ir al inicio de la disposición dónde se establece claramente *"Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica"*. Esto nos lleva a preguntarnos, ¿todas las previsiones de la Disposición Adicional 17.2, son un desarrollo de lo establecido en este artículo del Reglamento (UE) 2016/679?

Independientemente de la respuesta que podamos dar, en la práctica se trata de unos requisitos adicionales generales, también previstos por otras normas, que de forma indirecta les acabarán aplicando.

En este sentido también se pronuncia la APDCAT en su Dictamen 15/2019, como ya hemos apuntado anteriormente, para concluir que para que el tratamiento de los datos seudonimizados en base a lo establecido en el RGPD y la LOPD-GDD sea lícito, además deben cumplirse las garantías y cautelas que establece la normativa de protección de datos para el tratamiento de categorías especiales de datos. Así pues debemos hablar de unas obligaciones y medidas de seguridad generales a aplicar a cualquier tipo de categoría especial de dato, con independencia de la concurrencia del consentimiento o de otra habilitación legal que justifique su tratamiento.

En relación a este dictamen, ¿cómo se concreta en la práctica?

a) Obligación de realizar una evaluación de impacto. ¿En qué sentido se debe entender esta obligación? ¿El responsable del tratamiento debe

realizar una evaluación de impacto cada vez que se presente un proyecto de investigación al CEI?

En este sentido, a pesar de que la normativa no se pronuncia, parece lógico entender que si un investigador utiliza las herramientas proporcionadas institucionalmente para llevar a cabo un proyecto de investigación, y estas se han sometido a una evaluación de impacto sería suficiente con esta evaluación, no siendo necesario añadir el requisito de que cada proyecto presente su evaluación de impacto.

Por consiguiente debemos delimitar cuando pediremos una evaluación de impacto, ¿será por proyecto concreto, o podemos admitir una por centro?

Así pues el CEI, previa comprobación de que los datos del proyecto se han obtenido con base a cualquiera de los supuestos legales comentados, debe verificar que el proyecto cumple con este requisito.

Tal y como hemos explicado previamente, por el simple hecho de que se traten datos de categorías especiales de datos, debería hacerse la evaluación de impacto. Esta norma simplemente concreta que, aunque se trate de datos seudonimizados para su uso en investigación, también se debe hacer la evaluación de impacto.

Por otra parte, debe tenerse en cuenta que en mayo de 2019 la Agencia Española de Protección de datos ha publicado la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos[6]. Esta lista se basa en los criterios establecidos por el Grupo de Trabajo del Artículo 29 en la guía WP248 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD", especificando entre ellos los tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD.

b) Someterse a las normas de buena práctica clínica y de calidad aplicables.

En el ámbito de los ensayos clínicos por ejemplo debe tenerse en cuenta el cumplimiento de las normas de Buena Práctica Clínica (BPC).

[6] Disponible en: https://www.aepd.es/prensa/2019-05-06.html

c) Adoptar las medidas necesarias para que los investigadores no puedan acceder a datos identificados.

Una norma universal en investigación es que deber realizarse con datos codificados. Así mismo y de forma adicional, en el caso de la habilitación legal para el uso de datos para investigación, prevista en el artículo 89 del Reglamento (UE) 2016/679, los datos se deben seudonimizar.

Por lo tanto, podemos entender esta cautela en el sentido de que los datos se seudonimizan y los investigadores, a menos que concurran los supuestos legamente establecidos, no pueden acceder a los datos identificativos de los sujetos participantes en los estudios.

Este tercer requisito también es una buena práctica habitual que los investigadores venían cumpliendo hasta ahora. Lo único que variará en este punto es el grado de codificación o seudonimización de los datos en función de la base legal que se utilice para tratarlos.

d) Previsión de nombrar un representante legal en el territorio de la UE. Esta obligación tiene su base en la normativa de ensayos clínicos, cuando el Promotor del ensayo no tiene su sede en la UE.

Por consiguiente, este artículo viene a recoger y sistematizar las disposiciones que encontramos repartidas en la legislación en la materia, incluso más allá de la normativa de protección de datos y resulta aplicable a los casos previstos en el artículo 89 del RGPD.

8. Discusión

Antes de la publicación del Reglamento (UE) 2016/679 los investigadores se enfrentaban a serias dificultades para legitimar el uso de datos con fines de investigación mediante el consentimiento del paciente. Si bien existía la opción de anonimizar esto no siempre era posible porque restaba valor a la investigación, ya que con frecuencia es necesario recabar nuevos datos del sujeto.

Con la entrada en vigor del Reglamento (UE) 2016/679, y en especial de la Disposición Adicional 17 de la LOPD-GDD, se introducen nuevos supuestos y, conjuntamente con la interpretación de la normativa sectorial, se abren nuevas perspectivas para el uso de datos de salud y de tipo genético para

investigación biomédica, algunas con aplicación directa en el ámbito de la explotación masiva de datos, cómo el uso de datos seudonimizados.

El Reglamento General de Protección de Datos y la Ley española desarrollan una interpretación más flexible del alcance que puede darse al consentimiento, estableciendo bases jurídicas alternativas al consentimiento para el uso de datos de salud con fines de investigación biomédica.

La nueva LOPD-GDD, por ejemplo, señala que no será necesario que la persona preste su consentimiento para una investigación o rama concreta, sino que, teniendo en cuenta la interpretación derivada directamente del RGPD, se podrá otorgar el consentimiento para una finalidad amplia de investigación.

Por otra parte, no se requiere volver a recabar el consentimiento del sujeto fuente en el caso en el que se reutilicen datos para "finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial" (DA 17. 2. c), siempre y cuando se cumplan unas garantías adicionales mínimas, como atender al deber de información y transparencia y obtener el informe favorable previo del CEI. La misma regla es aplicable también para aquellas investigaciones iniciadas con anterioridad a la entrada en vigor de la Ley, tal y como recoge la Disposición Transitoria sexta, situación en la que no se han contemplado las garantías adicionales.

Finalmente es destacable que se admitiría la exención de solicitud de consentimiento cuando no sea posible la identificación de la persona por haber sido seudonimizados sus datos, cuando recabarlo sea imposible o suponga esfuerzos desproporcionados –en los supuestos de investigación de carácter general bajo una serie de requisitos adicionales–, y en situaciones de excepcional gravedad para la salud pública.

Es esperable que este nuevo marco regulatorio facilite la realización de proyectos de investigación en los que sea difícil o impracticable solicitar el consentimiento del titular de los datos.

9. Conclusiones

Como conclusiones podemos destacar que:

1. El Reglamento (UE) 2016/679 y la LOPD-GDD suponen una ampliación de los supuestos en los que se pueden utilizar los datos para investigación, pasando del esquema de la antigua normativa, donde o se disponía de un consentimiento expreso o se anonimizaban los datos para utilizarlos en investigación, a un nuevo esquema donde se amplía la base de la legitimación, y se supera el concepto del consentimiento. La legitimación no proviene de un solo factor, como es la norma o el consentimiento, sino de la combinación de diversos elementos que permiten garantizar, por un lado, que se respeta la intimidad y la autonomía de los pacientes, y por otro lado que favorece la investigación.

2. En cuanto a su ubicación, no parece que la regulación del uso de datos de salud deba hacerse a través de una disposición transitoria y una adicional. Falta una sistematización que facilite su interpretación. El redactado da pie a plantearse algunas dudas en cuanto a su interpretación, que ya hemos ido exponiendo a lo largo de este documento; incógnitas que es de esperar que futuras interpretaciones de las Autoridades de Protección de Datos competentes vengan a aclarar.

3. En cuanto a las formas de legitimar el uso de los datos en investigación, a día de hoy podemos afirmar que:

   a) Se admite el consentimiento por área de investigación. Este consentimiento debe entenderse como una forma expresa de dar el consentimiento, pero dentro de una misma línea o área puede permitir utilizar los datos de los sujetos para varios proyectos. Este consentimiento debe acompañarse de una correcta información al titular de los datos.

   b) Se admite la reutilización de los datos de proyectos de investigación preexistentes para ser utilizados en proyectos de investigación relacionados, siempre que se informe adecuadamente al titular de los datos del posterior uso y el proyecto se someta al dictamen del CEI. El régimen y condiciones de reutilización es diferente en función de si los datos se han recogido antes o después de la entrada en vigor de la LOPD-GDD, pero parece lógico pensar que, aunque los datos se hayan recogido antes de la entrada en vigor de la LOPD-GDD, también deba exigirse

que se informe al titular de los datos sobre su uso y el proyecto de someta al dictamen del CEI.

c) Podemos afirmar que los datos de las historias clínicas de los pacientes, por interpretación conjunta de la Ley 41/2002 y de la Disposición Adicional 17 de la LOPD-GDD, se podrán utilizar para investigación de forma seudonimizada, siempre que se cumplan los requisitos de la LOPD-GDD. Esto implica que concurra una separación entre el equipo investigador y quién realiza la seudonimización, y exista un compromiso de confidencialidad y de no reutilización de los datos. Debemos distinguir el concepto de seudonimización de codificación, ya que en el ámbito de la investigación siempre se deberán codificar los datos pero sólo en determinadas ocasiones se deberá seudonimizar.

d) En cuanto al uso de datos para investigación en materia de salud pública, la normativa admite llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

4. En el caso del tratamiento de datos genéticos, sería necesario modificar la LIB, así como la normativa reguladora de estudios observacionales, para incluir un capítulo sobre investigación con datos, integrando las implicaciones en los diferentes tipos de investigación sin medicamentos ni productos sanitarios.

5. En cuanto a las medidas adicionales, a tener en cuanta cuando se realice investigación en base al artículo 89 del Reglamento (UE) 2016/679, además de lo establecido en la LOPD-GDD, se deben seguir las buenas prácticas en investigación o el sometimiento del proyecto al dictamen de un CEI, que ya se encuentran en la normativa en otros ámbitos relacionados con la investigación.

6. Es muy importante que los centros de investigación tomen conciencia de las oportunidades que supone esta nueva regulación, que establezcan los mecanismos necesarios para la difusión y concienciación de las implicaciones de esta nueva normativa y que apliquen las medidas que les permita aprovechar estas novedades (p.ej. implantar consentimientos amplios para investigación conjuntamente con los consentimientos asistenciales y/o Acuerdos de Transferencia de Datos…).

7. Así mismo es fundamental que los CEI lleven a cabo las acciones necesarias para adaptarse a los cambios normativos que les va a suponer este cambio de paradigma (p.ej. necesidad de Delegado de protección de Datos o un experto con conocimientos suficientes del Reglamento (UE) 2016/679).

10. Bibliografía

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Reglamento (UE) 2016/679 del Parlamento y el Consejo Europeo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE.

Ley 14/2007, de 3 de julio, de Investigación Biomédica.

Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica.

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

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.

Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica.

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

Declaración Internacional sobre los Datos Genéticos Humanos de Naciones Unidas. Paris, 16 de octubre de 2003.

Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio de Oviedo), hecho en Oviedo el 4 de abril de 1997.

Dictamen 05/2014 sobre técnicas de anonimización adoptado el 10 de abril de 2014 por el Grupo de Trabajo sobre Protección de datos del Artículo 29.

Statement on Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU, adopted on 16 September 2014. Article 29 Data Protection Working Party.

Documento de trabajo sobre datos genéticos adoptado el 17 de marzo de 2004 por el Grupo del artículo 29 sobre protección de datos.

Marco de actuación para el uso compartido responsable de datos genómicos y relativos a la salud de la Alianza Global para la Genómica y la Salud. Versión de 10 de septiembre de 2014.

Código de Buenas prácticas en protección de datos para proyectos Big Data editado por la Agencia Española de Protección de Datos.

Web proyecto PADRIS: http://aquas.gencat.cat/ca/projectes/analitica_dades/

Web proyecto BIG DATIUS: http://www.bigdatius.com/

Informe 073667/2018 Agencia Española de Protección de Datos https://www.aepd.es/informes/juridicos/

Web AEMPS enlace modelo consentimiento informado para ensayos clínicos: https://www.aemps.gob.es/investigacionClinica/medicamentos/ensayosClinicos.htm

Dictamen Autoridad Catalana de Protección de Datos CNS 18/2019.

Dictamen Autoridad Catalana de Protección de Datos CNS 15/2019.

Dictamen 3/2019, sobre "Preguntas y Respuestas sobre la interrelación entre la regulación de ensayos clínicos y el RGPD" de 23 de enero de 2019, del Comité Europeo de Protección de Datos.

Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo*

Informative self-determination, validity of consent and protection of sensitive data: criticisms of the new regulatory framework

Profa. Dra. Inmaculada Vivas-Tesón

Profesora Titular de Derecho Civil en la Universidad de Sevilla (Sevilla, España)

DOI: 10.14679/1138

Sumario / Summary: 1. La era de los datos personales. 2. El derecho a la autodeterminación informativa. 3. Datos de salud y datos genéticos tras la entrada en vigor del Reglamento UE y la LOPDyGDD. 4. Validez del consentimiento para el tratamiento de datos sensibles. 4.1. La problemática en torno al menor maduro. 4.2. El derecho a la accesibilidad universal de la persona con discapacidad. 4.3. La persona con capacidad judicialmente modificada. Un breve apunte del Anteproyecto de ley de reforma de la legislación civil y procesal en materia de discapacidad. 5. Bibliografía.

* Artículo recibido el 6 de febrero de 2019 y aceptado para su publicación el 9 de junio de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos -*Big Data*-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER)". Asimismo, este trabajo se incluye entre los resultados del Proyecto "Discapacidad, Enfermedad Crónica y Accesibilidad a los Derechos" (DER2016-80138-R), así como del Grupo de Investigación SEJ617 "Nuevas dinámicas del Derecho privado Español y Comparado" encuadrado en la Consejería de Educación y Ciencia de la Junta de Andalucía.

Dirección de correspondencia: ivivas@us.es

Resumen / Abstract: La entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y de la nueva Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales, ha supuesto un antes y un después en cuanto a la toma de conciencia del valor de nuestros datos personales y de nuestra facultad de disponer y controlar su uso. Sin embargo, en relación a la problemática en torno al tratamiento de los datos clínicos y genéticos, las imprecisiones y dudas persisten. Cambia el nombre, no la sustancia.

The entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the new Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights, has meant a before and after in terms of becoming aware of the value of our personal data and our ability to dispose and control their use. However, regarding problems around the treatment of health and genetic data, the inaccuracies and doubts still persist. The name changes, but not the substance.

Palabras clave / Keywords:

Protección de datos / Datos de salud / Datos genéticos / Consentimiento válido.

Data protection / Health data / Genetic data / Valid consent.

1. La era de los datos personales

En el mundo globalizado y digital del Siglo XXI, nuestros datos personales se han convertido en una codiciada fuente de energía (renovable[1]). Son la base de la toma de decisiones y, por consiguiente, un recurso clave para el impulso del avance económico, científico y tecnológico, en definitiva, para la mejora de nuestras vidas y de nuestro entorno. Sin embargo, su tratamiento, uso y destino puede, en ocasiones, resultar nocivo para su titular cuando resulta violada su privacidad. Tal desnudo no consentido de su yo (ya sea personal o patrimonial) puede acarrearle consecuencias perjudiciales e irreparables.

En la nueva era tecnológica, nuestros datos personales son utilizados para conocer nuestra vida cotidiana, nuestros gustos en todos los ámbitos, dónde nos encontramos a través de la geolocalización, con quién nos relacionamos, cómo reaccionamos ante las noticias, nuestra salud, etc. Un servidor lo almacena todo, también lo que nosotros consideramos absolutamente irrelevante, como la edad, el sexo o la dirección de correo electrónico. Con nuestra información se puede prever, con alta probabilidad de éxito, nuestros

[1] A diferencia de otros recursos, los datos personales no se agotan una vez utilizados, por ello su carácter renovable, pudiéndose reutilizar combinándolos con otros conjuntos de datos.

comportamientos futuros e, incluso, qué patologías sufriremos. Pero también nuestra información genética es material imprescindible para el desarrollo de proyectos de investigación biomédica.

Nuestros datos se comparten, circulan como valiosas mercancías de relaciones comerciales o bien de relaciones profesionales no siempre dotadas, unas y otras, de la máxima seguridad. A nuestra información se accede, física o electrónicamente, con suma facilidad. Con distintas finalidades (económicas, científicas, judiciales, personales, mera curiosidad, etc.) se asoman a nuestras vidas infinidad de instituciones, empresas y personas sin que reparemos mínimamente en ello y, en muchas ocasiones, sin control alguno. Nuestra privacidad está en peligro y ello podría repercutir negativamente, entre otros, en el ámbito laboral y en el de seguros[2].

En España, no somos plenamente conscientes de la crucial importancia de la protección de datos y de los grandes riesgos que comporta la falta de garantías adecuadas ante injerencias no consentidas en nuestra vida privada. Nosotros mismos minusvaloramos nuestra privacidad. Ello puede ser debido al puro desconocimiento o también a que las intrusiones en nuestra esfera personal nos pasan inadvertidas (p. ej. llamadas telefónicas o envíos postales).

A finales del siglo pasado los países comenzaron a legislar sobre la materia, pero muy recientemente nos hemos dado cuenta de que nuestros datos nos pertenecen y que somos nosotros los titulares de la facultad de decidir, disponer y controlar su uso (y su mal uso).

En la preocupación por la llamada *data protection* mucho ha tenido que ver el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que

[2] Atendiendo a una fuerte reivindicación del movimiento asociativo, el legislador, mediante la Ley 4/2018, de 11 de junio, ha introducido, en la Ley 50/1980, de 8 de octubre, del Contrato de Seguro una Disposición Adicional 5ª con el siguiente tenor literal: "No se podrá discriminar a las personas que tengan VIH/SIDA u otras condiciones de salud. En particular, se prohíbe la denegación de acceso a la contratación, el establecimiento de procedimientos de contratación diferentes de los habitualmente utilizados por el asegurador o la imposición de condiciones más onerosas, por razón de tener VIH/SIDA u otras condiciones de salud, salvo que se encuentren fundadas en causas justificadas, proporcionadas y razonables, que se hallen documentadas previa y objetivamente". El texto normativo es prácticamente igual al de la Disposición Adicional 4ª, relativa a la no discriminación por razón de discapacidad añadida por Ley 26/2011, de 1 de agosto. Si bien los fines son muy loables, no tanto la técnica legislativa utilizada de introducir una disposición adicional por cada colectivo o situación que pueda ser objeto de estigmatización en la contratación de seguros.

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 (en adelante, Reglamento UE).

En general, ha habido un antes y un después tras la entrada en vigor de la norma europea de carácter directamente vinculante, la cual nos ha hecho abrir los ojos y reflexionar acerca del enorme valor de nuestros datos personales en un mundo *online*, si bien, en cuanto a la materia que centrará la atención de las próximas páginas, los datos particularmente sensibles o especiales (en terminología del Reglamento UE), los que han de gozar de una protección jurídica más intensa[3] con una actitud de vigilancia proactiva, lamentablemente, no ha supuesto grandes novedades. Pese al nuevo marco normativo y su innegable relevancia estratégica, como el propio lector comprobará, las imprecisiones y dudas persisten. Todo sigue prácticamente igual.

Si, de un lado, los dueños de datos tan delicados se sienten desprotegidos, de otro, están muchos profesionales del ámbito clínico y científico que se encuentran perdidos, inseguros en cuanto al tratamiento y uso de los mismos, como si caminaran sobre arenas movedizas.

Pese a ello, con el nuevo marco normativo, poco o nada ha cambiado. Cambia el nombre (en lugar de datos sensibles, el Reglamento UE pasa a denominarlos "especiales"), pero no la sustancia.

2. El derecho a la autodeterminación informativa

Como se ha puesto de manifiesto, el dato personal se ha convertido, hoy, en el metro de medida de un producto o servicio, razón por la cual es preciso un marco legal regulador del derecho del ciudadano a disponer de sus datos y a controlar el flujo de los mismos.

Tal derecho conecta con el de intimidad y respeto a la vida privada y familiar y, en última instancia, con la intangibilidad de la dignidad humana.

Hoy por hoy, si bien no se encuentra expresamente reconocido en nuestra Constitución (en lo sucesivo, CE) como sí, en cambio, en las de otros países

[3] Romeo Casabona, C. M., "Implicaciones jurídicas de la utilización de muestras biológicas humanas y biobancos en investigación científica", 2007, p. 27. Disponible en: http://www.catedraderechoygenomahumano.es/images/Informe_final_completo.pdf [Última consulta: 30 de agosto de 2019].

de nuestro entorno como la lusa[4], es unánime considerar que el derecho a la autodeterminación informativa tiene naturaleza de derecho fundamental[5] incardinado en el art. 18.4 CE.

Tras la tibieza mostrada, en un primer momento, por nuestro Tribunal Constitucional, como puede comprobarse en sus Sentencias 254/1993 (Sala Primera), de 20 julio y 94/1998, de 4 de mayo, en las cuales parece configurar el derecho a la protección de datos personales como un derecho autónomo respecto del de intimidad del art. 18.1 CE, no será hasta la Sentencia del Pleno 292/2000, de 30 de noviembre, cuando el Constitucional lo configure, con absoluta nitidez, como un derecho autónomo e independiente[6].

---

[4] Su art. 35, relativo a la utilización de la informática, reconoce: "1. Todos los ciudadanos tienen derecho a acceder a los datos informatizados que les conciernan, pudiendo exigir su rectificación y actualización, así como el derecho a conocer la finalidad a que se destinan, en los términos que establezca la ley.
2. La ley define el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección, especialmente a través de una entidad administrativa independiente.
3. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones filosóficas o políticas, afiliación a partidos o sindicatos, confesión religiosa, vida privada y origen étnico, salvo con el consentimiento expreso del titular, autorización prevista por la ley con garantías de no discriminación o para procesamiento de datos estadísticos no identificables individualmente.
4. Se prohíbe el acceso a datos personales de terceros, salvo en casos excepcionales previstos por la ley.
5. Se prohíbe la atribución a los ciudadanos de un número nacional único.
6. Se garantiza a todos el libre acceso a las redes informáticas de uso público, determinando la ley el régimen aplicable a los flujos de datos transfronterizos y las formas adecuadas de protección de datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional.
7. Los datos personales que consten en ficheros manuales gozan de protección idéntica a la prevista en los apartados anteriores, en los términos que establezca la ley".

[5] El Reglamento UE proclama, de manera explícita, en su Considerando 1º que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.

[6] Consistente en "un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién

De este modo, añade la Sentencia del Pleno núm. 39/2016, de 3 marzo, "el consentimiento del afectado es, por tanto, el elemento definidor del sistema de protección de datos de carácter personal. La LOPD establece el principio general de que el tratamiento de los datos personales solamente será posible con el consentimiento de sus titulares, salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento" (FJ 3º)[7].

Resulta curioso que, pese al descubrimiento muchos años después de 1978 de la autodeterminación informativa en el art. 18.4 CE como un derecho fundamental de nuevo cuño y autónomo del derecho a la intimidad, la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDyGDD) abra su Preámbulo presumiendo de que nuestra *Carta Magna* fue pionera al consagrar expresamente la protección de datos de carácter personal como un derecho fundamental[8].

---

dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.
En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos" (FJ 7º).

7 Acerca de la línea evolutiva seguida por el Tribunal Constitucional en sus diversos pronunciamientos hasta configurarlo como un derecho fundamental independiente, *vid*. Villaverde Menéndez, I., "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal", *La protección de datos de carácter personal en los centros de trabajo*, Farriols i Solá, A. (Coord.), Ed. Cinca, Madrid, España, 2006, pp. 48-63; Palomar Olmeda, A. / Pérez González, C., *La protección de datos: su marco constitucional y el contexto del nuevo Reglamento. Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre)*, 2008**;** y Hernández López, J.M., *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucion*al, Ed. Aranzadi, Cizur Menor, España, 2013.

8 "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos de carácter personal cuando dispuso que 'la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'. Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno".

El derecho a la protección de datos personales se reconoce explícitamente en el art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 16.1 del Tratado de Funcionamiento de la Unión Europea.

En nuestro país, la reciente LOPDyGDD reemplaza a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD), integrando, así, en nuestro ordenamiento jurídico, los principios y mandatos del esperadísimo Reglamento UE[9], el cual entró en vigor el 24 de mayo de 2016 y es aplicable, de forma directa[10], en todos los países UE desde el 25 de mayo de 2018, con independencia de que, para tal fecha y habiendo contado con un periodo transitorio de dos años, hubieran

[9] En el Derecho de la Unión destacamos 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 a la libre circulación de estos datos, el Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, así como la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.
Junto al Reglamento (UE) 2016/679, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión 1247/2002/CE, COM(2017) 8 final, así como la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM(2017) 10 final, actualmente en fase de negociación, dotará a la Unión Europea de un sólido conjunto normativo de protección de datos.
Por su parte, para la jurisprudencia europea, la protección de los datos de carácter personal, que resulta de la obligación expresa establecida en el art. 8.1 de la Carta de los Derechos fundamentales de la UE, tiene una importancia especial para el derecho al respeto de la vida privada consagrado en el art. 7 de aquélla, como ha reconocido en diversas ocasiones el Tribunal de Justicia Europeo. Por todas, *vid*. STJUE (Gran Sala) de 8 de abril de 2014, en el caso Digital Rights Ireland Ltd y otros (TJCE 2014, 104) y 13 de mayo de 2014, en el caso Google Spain S.L. contra Agencia Española de Protección de Datos.

[10] Art. 99 del Reglamento UE, de conformidad con lo dispuesto por el art. 288 del Tratado de Funcionamiento de la Unión Europea. *Vid*. Comunicación de la Comisión al Parlamento Europeo y al Consejo "Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018", de 24 de enero de 2018. Disponible en: https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-43-F1-ES-MAIN-PART-1.PDF [Última consulta: 30 de agosto de 2019].

introducido los pertinentes ajustes en sus Derechos nacionales. Nosotros hemos cumplido, pero extemporáneamente.

Pese a su dilatada gestación, iniciada en enero de 2012, el Reglamento UE, a través de unas bases y directrices únicas, tiene como principal objetivo, dado el aumento de los flujos de información transfronterizos[11], homogeneizar las distintas regulaciones de protección de datos personales y libre circulación de los mismos de los veintiocho (por ahora) Estados miembros[12], elevando, a escala europea, la tutela de los derechos de los ciudadanos en el interior de la Unión[13].

Se trata, por tanto, de crear un marco jurídico sólido y común para la obtención, gestión y uso de datos que salvaguarde las libertades y derechos fundamentales de la persona y, en particular, el derecho a la protección de los datos de carácter personal, lo que contribuirá a generar confianza en la ciudadanía acerca del control efectivo de la privacidad[14], redundando ello, cómo no, en beneficio del mercado único digital de la UE[15].

El Reglamento UE contiene conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46 pero, con una evidente pretensión garantista, introduce algunos aspectos novedosos, entre los cuales, podemos destacar los siguientes: deja de considerar el silencio o la inacción como un consentimiento válido (por tanto, no se admite el tácito o por omisión), exigiendo una clara acción afirmativa (un "SÍ") para expresar aquél (art. 7)[16]; refuerza derechos existentes e incorpora otros nuevos como

---

[11] Acerca de los flujos internacionales de datos personales, *vid*. Comunicación de la Comisión "Intercambio y protección de los datos personales en un mundo globalizado", COM(2017) 7 final, de 10 de enero de 2017. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0007 [Última consulta: 30 de agosto de 2019].

[12] Actualmente, las apreciables diferencias en el nivel de protección de los datos de carácter personal de las personas físicas en el seno de la UE son debidas a la existencia de divergencias en la transposición de la Directiva 95/46/CE por parte de los distintos Estados miembros.

[13] *Vid*. Considerando 10º del Reglamento UE.

[14] Considerando 7º del Reglamento UE.

[15] Para un detenido estudio, *vid*. Troncoso Reigada, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Núm. 43, Julio-Diciembre 2012; Herrán Ortiz, A.I., "Aproximación al derecho a la protección de datos personales en Europa: el Reglamento general de protección de datos personales a debate", *Revista de Derecho, Empresa y Sociedad*, Núm. 8, 2016, pp. 179-200; y Nogueira Blanco, J., "Reglamento General de Protección de Datos (RGPD) y big data", *Actualidad Civil*, Núm. 5, 2018.

[16] *Vid*. Considerando 32º del Reglamento UE.

el de transparencia de la información (art. 12), el de eliminación o "derecho al olvido" (art. 17) o el de portabilidad de los datos (art. 20); establece el principio fundamental de responsabilidad proactiva, en cuya virtud el responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento (art. 24); introduce la evaluación de impacto relativa a la protección de datos como nuevo instrumento para ayudar a evaluar el riesgo antes de que se inicie el tratamiento (art. 35); crea, con carácter novedoso, la figura del Delegado de Protección de Datos (arts. 37 a 39) y establece, con evidentes fines disuasorios, un severo régimen sancionador con multas administrativas a responsables y encargados del tratamiento (arts. 83 y 84)[17].

Consciente de que el derecho a la protección de datos personales no es un derecho absoluto, pudiendo existir puntos de fricción con otros derechos fundamentales y libertades públicas tales como la de expresión e información o el derecho a la tutela judicial efectiva, uno de los grandes retos que suscita esta nueva normativa europea es cómo alcanzar el justo equilibrio entre tratamiento y protección de datos, para lo cual ha de recurrirse al principio de proporcionalidad y alcanzar, ponderadamente, la solución más justa en cada caso concreto[18].

---

[17] Según el art. 83.5 del Reglamento UE, las multas pueden ascender hasta los 20.000.000 de euros o, en el caso de una empresa, hasta el 4% de su volumen de negocios anual a nivel mundial del ejercicio fiscal anterior.
Al respecto y en estrecha relación con las cuestiones objeto de nuestra atención, La Autoridad nacional portuguesa competente en materia de protección de datos ha impuesto a finales de 2018 una multa de 400.000 euros a un hospital por permitir el acceso indebido por parte de profesionales sanitarios a historias clínicas de pacientes sin su consentimiento expreso. Disponible en: http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/primera-multa-post-rgpd-en-portugal [Última consulta: 30 de agosto de 2019].

[18] "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística" (Considerando 4º del Reglamento UE).

Así las cosas, es evidente que la norma comunitaria ha introducido nuevas garantías para reforzar la tutela del derecho de autodeterminación informativa, intentando remediar la falta de homogeneidad entre las distintas legislaciones internas de los Estados miembros.

Si bien nuestra LOPD fue formulada en 1999 cuando ya había irrumpido en nuestras vidas el fenómeno internet, lo cierto es que la red, hace casi veinte años (inolvidable el desagradable pitido del módem al conectarse, así como la baja velocidad de navegación), aún no se había abierto al mundo a los niveles actuales y, por tanto, no suponía una nueva forma de amenaza para la dignidad y los derechos de la persona como, sin duda, lo es ahora.

El escenario virtual, en estos momentos, es muy distinto, incomparable con el que le precedió. Es en estos años de la imparable revolución digital, de las nuevas tecnologías de la información y comunicación (TICs), del espectacular crecimiento de las redes sociales (profesionales y de ocio), de la infinidad de sensores que captan información por doquier, de la generalización del uso de teléfonos móviles y ordenadores portátiles que permiten compartir datos o imágenes (propias o de terceras personas) con una inusitada rapidez, de las omnipresentes aplicaciones (apps) a las que accedemos cotidianamente desde diversos dispositivos electrónicos y del *Big Data*, cuando se ha comenzado a comprender el inmenso potencial que encierran los datos y a tomar conciencia acerca de la capital importancia de su protección (basta pensar en el grave perjuicio que para la vida del ciudadano en sociedad puede tener una fuga de información sensible[19], como la relativa a la salud, en el ámbito laboral o de la contratación de seguros), de modo que la seguridad y transparencia de su tratamiento y uso han pasado a un primer plano, convirtiéndose en un objetivo prioritario y estratégico, un verdadero reto o desafío. El volumen de información generada y almacenada por las distintas herramientas tecnológicas es elevadísimo y múltiples son sus usos, sus bondades, pero también sus riesgos, lo cual conlleva transcendentales implicaciones jurídicas.

Situados en este nuevo contexto, quisiéramos poner de relieve la singularidad que los datos genéticos presentan respecto de la información clínica, pues no es posible afirmar que el derecho a la autodeterminación informativa

[19] En opinión de Chieffi, "è stata proprio la precipua sensibilità dei dati sanitari, oltre che di quelli genetici, a indurre il legislatore europeo a rafforzare, mediante il ricorso ad una fonte regolamentare, il diritto dell'individuo a autodeterminare il proprio corpo e le informazioni che gli appartengono". Chieffi, L., "La tutela della riservatezza dei dati sensibili: le nuove frontiere europee", *federalismi.it*., Núm. 4, 2018, p. 21.

en relación a aquéllos pertenezca exclusivamente a una persona, quien no tiene poder soberano de disposición y control de tales datos pues éstos son de titularidad conjunta de todos los que integran una misma línea biológica: la "familia biológica", de la cual no forman parte el cónyuge o pareja de hecho ni los hijos adoptivos y sí, en cambio, integran terceras personas como los donantes de gametos. De este modo, la familia alcanza una dimensión física por consanguinidad, muy alejada del mundo de los afectos, de los sentimientos y del deseo de compartir un proyecto de vida en común para ceñirse al mero vínculo por estrictos lazos de sangre[20].

3. Datos de salud y datos genéticos tras la entrada en vigor del Reglamento UE y la LOPDyGDD

Nuestra privacidad debe ser especialmente protegida cuando entramos en contacto con servicios sanitarios o bioinvestigadores.

Lamentablemente, el Reglamento europeo no contiene una disciplina específica para el tratamiento de datos personales en el ámbito sanitario e investigador[21].

---

[20] Como sosteníamos en nuestro trabajo: Vivas-Tesón, I., "Uso y control de la información genética: dudas y retos para el Derecho privado", *Revista de Derecho Privado*, Núm. 5, Septiembre-Octubre 2016, p. 47.

[21] En su considerando 33, el legislador comunitario reconoce que "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida".
En el 34 define los datos genéticos: "Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente".
Y en el 35 afirma que "Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal,

Ya en el texto articulado de la norma, se definen los datos genéticos como aquellos "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona" en tanto que datos relativos a la salud son los "relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud", según las letras 13) y 15) de su art. 4, respectivamente.

Tanto los clínicos como los genéticos son considerados por el art. 9 del Reglamento UE como categorías especiales (si bien en el Considerando 51 se refiere a ellos como "particularmente sensibles") de datos personales al revelar la información más reservada de la persona, por ello que reciban una protección reforzada. El precepto sanciona como principio general la prohibición de tratar datos genéticos y datos relativos a la salud (apartado 1º), si bien, a continuación, levanta el veto cuando concurran circunstancias específicas, legitimando, en tales supuestos, el tratamiento de los mismos (apartado 2º).

La norma europea, en su art. 9.4, contempla que los Estados miembros puedan mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, añadiendo en su Considerando 53 *in fine*: "(…) No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos". Por tanto, el Reglamento UE, dados los márgenes de discrecionalidad que, a partir de los principios establecidos por el legislador europeo como mínimo común denominador, concede a los Estados miembros (el nuestro, como de inmediato se comprobará, no se ha esforzado mínimamente), no pretende introducir una disciplina uniforme en relación a la protección de los datos de salud y datos genéticos, persistiendo la fragmentación normativa a lo largo de todo el territorio comunitario, con las importantes consecuencias que de ello se derivan.

---

incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

Pese a ser indispensable la intervención del legislador español al respecto, la regulación del tratamiento de datos para fines sanitarios y de investigación en nuestra LOPDyGDD deja mucho que desear, pues tan sólo les dedica su Disposición adicional séptima, que se remite a las letras g), h), i) y j) del art. 9.2 del Reglamento europeo, las cuales contemplan la posibilidad de tratamiento de aquéllos por razones de interés público esencial, para fines de medicina preventiva o laboral, por razones de interés público en el ámbito de la salud pública y con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, respectivamente. La nueva norma no sólo no añade nada nuevo a lo disciplinado por el Reglamento europeo, sino que, sin más, se remite a él.

Sorprende sobremanera que, no obstante tratarse de una materia tan delicada y ser urgentes las medidas normativas de garantía y seguridad para los profesionales del ámbito sanitario e investigador, pero, sobre todo, para los interesados, hoy sigamos contando con una deficiente, inconexa y ambigua regulación.

El uso de nuestros datos de salud y genéticos para fines científicos presenta ciertas peculiaridades dignas de especial atención: no se trata de datos cualquiera, sino de datos "supersensibles"; el creciente interés de la comunidad científica por la información sanitaria y genética para lograr avances y mejorar nuestras condiciones de vida; la insuficiencia del deber de confidencialidad del profesional como garantía de protección de los datos; la imposibilidad de informar *a priori* de los posibles accesos y usos de tales datos; la nueva realidad del *Big Data*; los daños irreparables de una frágil protección ante la criminalidad informática (recordemos los estragos del *ransomware WannaCry* en el servicio sanitario británico hace unos meses) y del uso impropio de tales datos[22].

Los derechos y principios a tutelar tienen, todos, rango constitucional. A ello se suma que el nuevo contexto digital de *data protection* plantea problemas jurídicos nuevos que inciden en la relación entre privacidad e investigación científica y en la necesidad de colocar el fiel de la balanza. No puede pasarse por alto la función social que el Reglamento UE reconoce explícitamente al tratamiento de los datos personales en su Considerando 4, subrayando que carece de carácter absoluto cuando concurre con otros derechos fundamentales, con los cuales deberá ser reconciliado en virtud del principio de proporcionalidad. A propósito de ello, la interlocución entre

[22] De tales riesgos y perjuicios para los derechos y libertades fundamentales es consciente el legislador comunitario en el Considerando 75 del Reglamento europeo.

los juristas (preocupados por el respeto a los derechos de la persona) y la comunidad científica (para la que resulta indispensable la celeridad y la menor burocracia posible que comprima la libertad investigadora[23]) no siempre es fluida[24].

Así las cosas, consideramos que el tratamiento de los datos clínicos y genéticos precisa, en España, un desarrollo normativo específico que sea adecuado y satisfactorio tanto para la complejidad de aquél como para el incesante progreso científico y tecnológico. Esta materia requiere un marco normativo más sólido y coherente que genere confianza, parafraseando el Considerando 7 del Reglamento europeo.

4. Validez del consentimiento para el tratamiento de datos sensibles

En materia de protección de datos de carácter personal la relevancia del consentimiento es indiscutible.

Si bien solemos acompañar al consentimiento únicamente del calificativo "informado", éste debe ser igualmente libre y revocable, según el art. 5 del Convenio de Oviedo para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina de 1997[25].

---

[23] A propósito de la incidencia del Reglamento UE en los *Big Data* genéticos, *vid*. Quinn, P. / Liam, Q., "Big genetic data and its big data protection challenges", *Computer Law & Security Review*, Núm. 5, Vol. 34, Octubre 2018, pp. 1000-1018.

[24] Como sosteníamos en nuestro trabajo, Vivas-Tesón, I., "Uso y control de la información genética: dudas y retos para el Derecho privado", *op. cit*., p. 46, "estamos, sin duda, ante escenarios y horizontes completamente nuevos y con múltiples implicaciones (éticas, sociales, científicas, jurídicas, etc.), por tanto, de suma complejidad. Se trata de una materia en la que confluyen disciplinas filosóficas, jurídicas, antropológicas y científicas, entre las cuales el diálogo no siempre es todo lo fluido que sería deseable y los confines entre ellas son, con enorme frecuencia, difíciles de trazar. En este sentido, es preciso destacar que entre Ciencia y Derecho no existe siempre una recíproca comprensión". Además, continuábamos afirmando en p. 47, "el Derecho va avanzando, pero poco a poco y de forma claramente descompasada: Derecho y Ciencia caminan a dos velocidades distintas".

[25] Art. 5: "Una intervención en el ámbito de la sanidad sólo podrá efectuarse después de que la persona afectada haya dado su libre e informado consentimiento.
Dicha persona deberá recibir previamente una información adecuada acerca de la finalidad y la naturaleza de la intervención, así como sobre sus riesgos y consecuencias.
En cualquier momento la persona afectada podrá retirar libremente su consentimiento".

Teniendo muy presente lo anterior, para prestar válidamente el consentimiento al tratamiento de datos sensibles se requiere capacidad, la cual nos conduce a detenernos en tres situaciones: minoría de edad, discapacidad y capacidad judicialmente modificada.

Tanto los profesionales sanitarios como los comités de ética sienten, en la práctica diaria, una gran inseguridad jurídica en relación al consentimiento para el tratamiento de datos clínicos de personas no plenamente capaces en cuanto pacientes o sujetos fuente de la muestra biológica para investigación.

Además de las numerosas dudas jurídicas al respecto de las cuales daremos, de inmediato, oportuna cuenta, debemos tener presente el escenario tecnológico y científico actual (muy distinto al de hace unas décadas) así como los horizontes futuros. Sin poder adentrarnos, como sería deseable, en uno y otros, tan sólo nos limitamos a destacar el enorme impacto del *Big Data* en el campo de la salud, en el que, muy previsiblemente, sus aplicaciones crecerán de manera espectacular, tanto para el área médica, como también para las de análisis de datos (historias médicas, análisis clínicos…), la gestión de centros de salud, la administración hospitalaria y la documentación científica (generación, almacenamiento y explotación), con las consiguientes implicaciones y desafíos para el Derecho de la persona y la tutela de sus derechos[26].

[26] Vivas-Tesón, I., "Uso y control de la información genética: dudas y retos para el Derecho privado", *op. cit.*, pp. 47-48, "el estatuto jurídico de la persona se ha transformado profundamente en los últimos decenios, lo que ha obligado a abandonar la instrumentación patrimonialista de las categorías jurídicas, las cuales ya no pueden seguir reconduciéndose a los dos tradicionales pilares del Derecho privado: la propiedad y al contrato.
Baste pensar que el consentimiento en la cesión y utilización de la información genética nada tiene que ver con el consentimiento contractual. Las elecciones vitales de la persona y la consiguiente toma de decisiones en el campo biogenético no pueden incardinarse, sin más, en el régimen jurídico de la prestación del consentimiento para celebrar una compraventa, una donación o un préstamo. Las partes del cuerpo humano y la integridad genética de la persona no tienen carácter patrimonial ni en vida ni tras su muerte. Consentimiento informado, voluntades anticipadas, autotutela, renuncia a tratamientos sanitarios, etc. son actos jurídicos que no tienen por objeto una *res* del patrimonio de la persona que expresa la voluntad, sino la persona misma. Si en las relaciones contractuales el *favor commercii* puede llegar a sacrificar la voluntad contractual en aras de la seguridad del tráfico, en el campo de los valores personales es preciso favorecer todo lo posible la efectividad del consentimiento, el cual debe ser prestado por la propia persona y no por terceros que decidan por ella. La autonomía privada patrimonial difiere considerablemente de la autonomía personal o existencial, de modo que ésta no puede someterse al régimen jurídico de aquélla".

4.1. La problemática en torno al menor maduro

El menor de edad no emancipado es un sujeto especialmente importante y no jurídicamente fácil, aunque, a simple vista, pudiera parecerlo.

Y ello porque, de un lado, nuestras normas son profundamente adultocéntricas (desde 2015, más todavía, si cabe) y, por tanto, muy alejadas de la realidad que precisamente tratan de regular y, de otro, por su progresiva madurez para tomar decisiones de forma autónoma, la cual es tenida en cuenta por el legislador para posibilitarle o no la realización por sí solo de ciertos actos jurídicos.

El menor tiene exactamente los mismos derechos y libertades que todas las demás personas. No son ciudadanos de segunda clase. En materia de derechos humanos y libertades fundamentales es inadmisible una jerarquía o clasificación de personas. Necesitamos cambiar la forma de mirar y tratar a los niños, niñas y adolescentes como futuros adultos subordinados a los que ya lo son y pretenden someterlos a su autoridad.

Teniendo muy presente su plena ciudadanía, la preocupación por dotar al menor de edad de un adecuado marco legal de protección, dada su especial vulnerabilidad, trasciende de un amplio catálogo de Instrumentos Internacionales y Regionales (entre otros, la Declaración Universal de Derechos Humanos, los arts. 23 y 24 del Pacto Internacional de Derechos Civiles y Políticos y el art. 10 del Pacto Internacional de Derechos Económicos, Sociales y Culturales), pero muy especialmente, de la Convención ONU de los derechos del niño, adoptada y abierta a la firma y ratificación por la Asamblea General en su Resolución 44/25, de 20 de noviembre de 1989 (el Estado español la ratificó en 1990), la cual, de carácter vinculante, marca el inicio de una filosofía completamente nueva en relación con el menor de edad, basada en el relevante papel que desempeña en la sociedad y en la exigencia de un mayor protagonismo.

La Convención de los derechos del niño ha sido el primer Tratado que se ha ocupado específicamente de los derechos de la infancia, creando una nueva visión de los niños, niñas y adolescentes, considerados poseedores de derechos y responsabilidades apropiados a su edad y no una propiedad de sus padres. La persona menor de edad deja de ser vista como una simple receptora de atención y protección para pasar a ser considerada como un verdadero sujeto de derecho o agente de cambio. Los niños (no sólo los

adultos) son personas portadoras de derechos fundamentales[27], si bien, dada su indefensión, necesitan de un especial amparo para afrontar su desarrollo integral[28].

El Instrumento internacional (su incuestionable relevancia en el ámbito de la infancia y la adolescencia lo han hecho merecedor de la expresión *Carta Magna*) parte de cuatro principios fundamentales de carácter transversal: no discriminación (art. 2), el interés superior del menor (art. 3)[29], derecho a la supervivencia y al desarrollo del niño (art. 6) y la participación activa y respeto de la opinión del menor (art. 12). La Convención, como no podía ser de otra

---

[27] De esta opinión, Bosisio: "grazie ai nuovi orientamenti sull'infanzia, infatti, nei quali si attribuisce ai bambini un ruolo attivo nel processo di sviluppo, oggi i bambini e gli adolescenti non sono più considerati i meri destinatari del dovere degli adulti di proteggerli e di soddisfare i loro bisogni fondamentali, bensì titolari di diritti specifici". Bosisio, R., "La percezione dei diritti nell'infanzia e nell'adolescenza. Una ricerca empirica", *Sociologia del Diritto*, Núm. 1, 2005, p. 137.

[28] La Convención contiene 54 artículos, los cuales contemplan todo el conjunto de derechos civiles, políticos, económicos, sociales y culturales relacionados con la infancia, garantizando, especialmente, la personalidad individual del niño, su libertad de expresión, religión, asociación y asamblea y su derecho a la intimidad. Se ofrece, por tanto, una protección integral de la persona menor de edad**.**

En 2000, fueron añadidos dos Protocolos facultativos para ampliar la protección de la infancia en dos aspectos específicos: el relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía y el protocolo sobre la participación de niños en los conflictos armados.

[29] Al respecto, repárese que la Observación general Nº 14 (2013) sobre el derecho del niño a que su interés superior sea una consideración primordial (artículo 3, párrafo 1), subraya el concepto tridimensional del interés superior del menor: un derecho sustantivo, un principio jurídico interpretativo y una norma de procedimiento. En este sentido, contempla expresamente que "el artículo 3, párrafo 1, de la Convención sobre los Derechos del Niño otorga al niño el derecho a que se considere y tenga en cuenta de manera primordial su interés superior en todas las medidas o decisiones que le afecten, tanto en la esfera pública como en la privada".

Destacamos la nueva redacción del art. 2 de la Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, por la Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, para, como afirma en su Exposición de Motivos, reforzar el derecho del menor a que su interés superior sea prioritario. Sin embargo, permítasenos poner de relieve que el interés superior del menor pasa a quedar regulado en un precepto, nada más y nada menos, que de dos páginas de extensión (por otra parte, injustificadas), lo que, a nuestro entender, dificulta la interpretación y aplicación de la norma por parte del operador jurídico.

Para un detenido análisis del nuevo art. 2, *vid*. Guilarte Martín-Calero, C., "El interés superior del niño: la nueva configuración del artículo 2 de la Ley Orgánica, de 15 de enero, de protección jurídica del menor", Cabedo Mallol, V.J. / Ravetllat Ballesté, I. (Coords.), *Comentarios sobre las Leyes de reforma del sistema de protección a la infancia y la adolescencia*, Ed. Tirant lo Blanch, Valencia, España, 2016, pp. 87-129.

manera, no hace distingos, de modo que todos y cada uno de sus artículos se aplican igualmente a los niños y niñas con capacidades divergentes o diversamente capaces[30], a quienes reconoce el derecho al disfrute de una vida plena y decente (art. 23)[31] y a quienes también se aplica otro Tratado internacional, la Convención ONU de los derechos de las personas con discapacidad hecha en Nueva York el 13 de diciembre de 2006, otro hito normativo que ha supuesto un auténtico cambio de paradigma y que, por cuanto ahora nos ocupa, reconoce que los niños y las niñas con discapacidad deben gozar plenamente de todos los derechos humanos y libertades fundamentales en igualdad de condiciones con los demás niños y niñas (art. 7), prohibiéndose toda discriminación por motivos de discapacidad (art. 5).

Los Estados que han ratificado ambos Tratados internacionales tienen la obligación de crear las condiciones e instrumentos para que los derechos de los niños y niñas, sin excepción, sean respetados y que la tutela de los mismos no sea meramente nominal[32], removiendo todos los obstáculos que les impidan su pleno disfrute[33].

Partiendo de la consideración del menor como un sujeto vulnerable, el Reglamento UE, en su Considerando 38, asevera que "los niños [no compartimos el término empleado para traducir la norma al castellano] merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales".

---

30 En este sentido se pronuncia la Observación General del Comité de los Derechos del Niño nº 9 (2006) "Los derechos de los niños con discapacidad": "5 ...reconociendo la importancia de los artículos 2 y 23 de la Convención, el Comité afirma desde el principio que la aplicación de la Convención con respecto a los niños con discapacidad no debe limitarse a esos artículos.
6. La presente observación general tiene por objeto ofrecer orientación y asistencia a los Estados Partes en sus esfuerzos por hacer efectivos los derechos de los niños con discapacidad, de una forma general que abarque todas las disposiciones de la Convención...".

31 La Convención de los derechos del niño utiliza el término "impedidos", hoy día inaceptable por y carga peyorativa pero justificado en la fecha del tratado internacional.

32 Recuérdese que el art. 39.4 de la Constitución española dispone que "los niños gozarán de la protección prevista en los Acuerdos internacionales que velan por sus derechos", lo que, asimismo, es recogido por el art. 3 de la Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

33 En este sentido, para Picontó Novales, "el avance en el reconocimiento y desarrollo de mecanismos de protección de los derechos de los niños y adolescentes tiene todavía muchas tareas pendientes si se quiere pasar del reconocimiento a la efectividad de sus derechos". Picontó Novales, Mª.T., "Derechos de la infancia: Nuevo contexto, nuevos retos", *Derechos y Libertades*, Núm. 21, 2009, p. 59.

En Derecho español, el menor de edad no emancipado (sorprende cómo el legislador sólo en pocas ocasiones distingue expresamente cuándo el sujeto de sus normas es un menor no emancipado y cuándo emancipado y, por consiguiente, sin representación legal alguna) se caracteriza por tener una capacidad limitada, por ello que requiera una representación legal para la realización de los actos jurídicos (a excepción de los contemplados en el art. 162 C.c.), en concreto, patria potestad o tutela, sistemas de guarda que han de ejercerse siempre en interés superior del menor (art. 2 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor –en adelante, LOPJM–, precepto modificado en 2015), de acuerdo con su personalidad y con respeto a sus derechos, su integridad física y mental (art. 154 C.c.). Además, el Ministerio Fiscal tiene encomendada su protección y defensa (art. 3 del Estatuto del Ministerio Fiscal).

En este sentido, en nuestro ordenamiento se parte de la premisa de que el menor de edad no tiene aptitud suficiente para actuar jurídicamente, si bien se considera que es tendencialmente capaz, razón por la cual se le reconoce la posibilidad de realizar, por sí mismo (por consiguiente, sin ser sustituido por su representante/s legal/es), actos tanto en la espera personal como en la patrimonial.

Sin embargo, las normas que posibilitan su actuación completamente autónoma utilizan criterios dispares para los distintos actos jurídicos y, además, unos de carácter objetivo y otros de índole puramente subjetiva: para algunos actos la edad (12[34], 14[35] o 16[36] años), para otros la madurez suficiente[37] (el "madurómetro", permítasenos el término, aún no existe, de modo que surge el problema de a quién compete el juicio de si se trata o no de un menor maduro con el discernimiento necesario para el acto en cuestión). Todo ello crea una enorme confusión y grandes dificultades en la práctica cotidiana, en la que, aun en los casos en los cuales resulta preceptivo, no suele oírse y escucharse al menor en la toma de decisiones que le afectan (art. 9 LOPJM).

A lo anterior ha de sumarse la dispersión normativa, la abundancia de conceptos jurídicos indeterminados, las numerosas imprecisiones legales, los vaivenes legislativos según la sensibilidad ideológica de quien gobierna y la

[34] Por ejemplo, debe prestar su consentimiento para ser adoptado.

[35] Puede, entre otros actos, otorgar testamento (salvo el ológrafo) u optar por la nacionalidad o vecindad civil.

[36] Puede emanciparse y contraer matrimonio.

[37] Suficiente madurez para ser oído y escuchado en todas las decisiones que le afecten, en cuanto a los actos relativos a los derechos de la personalidad o para declarar como testigos.

ausencia de respuesta legal a numerosos interrogantes que surgen cada día en el ámbito sanitario y de la investigación, trasladándose al profesional una problemática, en muchas ocasiones, difícil de gestionar.

Lo expuesto se observa, con suma facilidad, en relación a la regulación de la prestación del consentimiento informado del menor de edad y del tratamiento de sus datos personales, muy especialmente, los sensibles, como son los relativos a su salud y genética.

Siguiendo un orden cronológico y sin ánimo de exhaustividad, la Ley 30/1979, de 27 de octubre, sobre extracción y trasplante de órganos exige que para obtener órganos procedentes de un donante vivo éste debe ser mayor de edad (art. 4).

La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en lo sucesivo, LAP), tras su modificación por la Ley Orgánica 11/2015, de 21 de septiembre, establece la mayoría de edad sanitaria en los 16 años, salvo cuando se trate de una actuación de grave riesgo para la vida o salud del menor, según el criterio del facultativo, en cuyo caso el consentimiento lo prestará el representante legal del menor, una vez oída y tenida en cuenta la opinión del mismo (art. 9.4)[38]. Recuérdese que a esta norma remite la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo, la cual, en su redacción anterior a 2015, permitía que las menores de 16 y 17 años pudieran decidir por sí mismas, debiendo sólo informar a uno de los dos titulares de la patria potestad o tutor, salvo que ello les produjese a la menor un conflicto grave[39].

---

[38] Para un detenido estudio, *vid*. Andreu Martínez, Mª. B., *La autonomía del menor en la asistencia sanitaria y el acceso a la historia clínica*, Ed. Aranzadi, Cizur Menor, Navarra, España, 2018, pp. 41-60; y De Montalvo Jääskeläinen, F., *Menores de edad y consentimiento informado*, Ed. Tirant lo Blanch, Valencia, España, 2019.

[39] El apartado 4º del art. 13 de la citada Ley, suprimido en 2015, rezaba así: "Cuarto.- En el caso de las mujeres de 16 y 17 años, el consentimiento para la interrupción voluntaria del embarazo les corresponde exclusivamente a ellas de acuerdo con el régimen general aplicable a las mujeres mayores de edad.
Al menos uno de los representantes legales, padre o madre, personas con patria potestad o tutores de las mujeres comprendidas en esas edades deberá ser informado de la decisión de la mujer.
Se prescindirá de esta información cuando la menor alegue fundadamente que esto le provocará un conflicto grave, manifestado en el peligro cierto de violencia intrafamiliar, amenazas, coacciones, malos tratos, o se produzca una situación de desarraigo o desamparo".

Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida, requiere mayoría de edad para ser usuario o receptor de las mismas, así como para ser donantes de material genético.

El art. 1 de la Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas exige mayoría de edad para solicitarla, de manera que aquélla reservada, exclusivamente, a los adultos (incluso las personas menores de edad emancipadas quedan excluidas del ámbito subjetivo de la Ley, pese a que nuestro Código civil (en adelante, C.c) tan sólo les establece restricciones de índole patrimonial). Ello confirma el enfoque adultocéntrico (además de binario) al que nos tiene acostumbrado nuestro legislador a la hora de elaborar las normas, olvidándose de normar bajo un prisma estrictamente existencial. Precisamente ello ha conducido a la Dirección General de los Registros y del Notariado a dictar la reciente Instrucción de 23 de octubre de 2018, con la cual intenta atender una realidad existente antes de los 18 años.

Por su parte, la Ley 14/2007, de 3 de julio, de Investigación Biomédica (en lo sucesivo, LIB), la cual parte del carácter excepcional de la investigación con muestras procedentes de menores de edad *ex* arts. 4.2 y 20.1 LIB (cuando "no existan otras alternativas para la investigación", si bien acto seguido, en su art. 20.2 LIB, relaja considerablemente dicha excepcionalidad en una serie de supuestos) exige, en caso de que el sujeto fuente sea menor de edad, el otorgamiento del consentimiento por terceros, sus representantes legales (art. 4.2), quienes "tendrán en cuenta los deseos u objeciones previamente expresados por la persona afectada" *ex* art. 20.1.d) LIB[40].

Ahora bien, la LIB parece dejar abierta la posibilidad de que el consentimiento sea otorgado por el propio menor de edad, sin intervención de sus representes legales, cuando "existan garantías sobre el correcto consentimiento", según dispone en su art. 58.5, letra d). De la ambigua letra de la ley surgen, de inmediato, algunos interrogantes: ¿cuáles son dichas garantías y quién determina la concurrencia de las mismas?; ¿podría entenderse que existe una remisión tácita al art. 9.3 LAP (de aplicación supletoria según la Disposición Final 2ª de la LIB[41]), precepto que prevé que los menores mayores

[40] Sobre la materia, *vid*. AA.VV., *Menores e investigación biomédica*, Gómez Sánchez, Y. (Coord.), Ed. Dykinson, Madrid, España, 2018.

[41] Disposición final 2ª. Aplicación supletoria. "En lo no previsto en esta Ley serán de aplicación la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, siempre que no sea incompatible con los principios de esta Ley, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

de 16 años puedan consentir las intervenciones médicas? Dada la falta de disposición expresa por parte del legislador, nos inclinamos por esta última solución por ser la más respetuosa con la voluntad del menor maduro, si bien nos sorprende por qué la LIB no lo ha previsto así explícitamente, la cual ni siquiera ha contemplado la obligación de los representantes legales de oír y escuchar al menor antes de tomar la decisión, la cual es impuesta, con carácter general, por el art. 9 LOPJM y art. 154 C.c. (el cual dice expresamente "siempre"), conformándose con la tímida previsión de que aquéllos tengan en cuenta "los deseos u objeciones previamente expresados por la persona afectada".

Un dato que nos hace sospechar que el legislador sólo piensa, en el contexto de la bioinvestigación, en el consentimiento por representación es que la LIB se preocupa únicamente por la accesibilidad de la información que ha de proporcionarse a las personas con discapacidad (arts. 4.1, pfo. 3º y 15.1), sin hacer la más mínima mención al formato adecuado de aquélla para los menores de edad, lo que confirma que éstos no son sus destinatarios.

Por cierto, tanto la LIB como el Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica (en adelante, RD 2011) obvian por completo a los menores emancipados, quienes, en atención a su estado civil, carecen de representantes legales y, por consiguiente, en este ámbito, deben ser equiparados a los mayores de edad a los efectos de prestar el consentimiento por sí mismos.

Una vez consentida la cesión de la muestra biológica con fines de investigación, la LIB reconoce al menor su participación "en la medida de lo posible y según su edad y capacidades en la toma de decisiones a lo largo del proceso de investigación" (art. 4.2 *in fine*), si bien el legislador no concreta la forma, grado y valor de aquélla. Ello nos lleva a distinguir entre "proceso de obtención del consentimiento" (por representación) y "proceso de investigación" (con participación directa del menor, la cual se desconoce por completo). Y nos hacemos una pregunta: en la práctica, ¿se involucra al menor de edad "a lo largo del proceso de investigación"? Por otra parte, ¿realmente el legislador está contemplando que el menor participe por sí mismo en el proceso de investigación antes de alcanzar la

mayoría de edad o sólo a partir de ésta? Nos lo preguntamos tras leer el art. 32.3 del RD 2011[42].

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la hoy derogada Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su art. 13.1, contempla que podrá procederse al tratamiento de los datos de los mayores de 14 años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de 14 años se requerirá el consentimiento de los padres o tutores.

La edad de 14 años está en armonía con lo dispuesto en el art. 8 del Reglamento UE, el cual, en relación al tratamiento de datos del menor en los servicios de la sociedad de la información, fija la edad para prestar el consentimiento en 16 años, si bien permite que los Estados miembros puedan establecer por ley una edad inferior a tales fines, siempre que ésta no sea inferior a 13 años. Recuérdese que a pesar de que el art. 8 del Anteproyecto de Ley Orgánica de protección de datos de carácter personal rebajó la edad para consentir el tratamiento de datos de carácter personal de los 14 a los 13 años (suponemos que ello encontraba justificación en la necesaria equiparación con las legislaciones de otros Estados miembros)[43], la reciente LOPDyGDD sigue manteniéndola en 14 (art. 7.1). En definitiva, el menor de edad de 14 años puede prestar, por sí mismo, su consentimiento para el tratamiento de sus datos personales. Por cierto, dado que los niños merecen una protección específica, como reconoce expresamente el Reglamento UE, nos parece todo un acierto que contemple en su Considerando 58 que "cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender", previsión que, por desgracia, nuestra LOPDyGDD no ha reproducido.

Por su parte, el Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la

---

[42] Dispone que "en el caso de utilización de muestras de menores de edad con fines de investigación biomédica, según lo previsto en el artículo 58.5 de la Ley 14/2007, de 3 de julio, el biobanco y las personas responsables de la colección o del proyecto de investigación tendrán la información a la que se refiere el apartado 1 de este artículo a disposición de la persona representante legal del sujeto fuente hasta que éste alcance la mayoría de edad, y del propio sujeto fuente a partir de ese momento".

[43] Disponible en: http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%A2%7F%8B%99tt%84sm%A3%91 [Última consulta: 30 de agosto de 2019].

Investigación con medicamentos y el Registro Español de Estudios Clínicos, contempla en su art. 5.3 que será necesario que se haya obtenido el consentimiento informado previo de los padres que no estuvieran privados de la patria potestad o del representante legal del menor, a quien deberá oírse si, siendo menor de 12 años, tuviera suficiente juicio. Cuando las condiciones del sujeto lo permitan y, en todo caso, cuando el menor tenga 12 o más años, deberá prestar además su consentimiento para participar en el ensayo. Por consiguiente, consentimiento por representación junto a consentimiento del menor con 12 años, elevación de edad y requisitos que puede encontrar justificación en el carácter experimental que conlleva un ensayo clínico.

En 2015, se introdujeron modificaciones importantes en el Código penal (en lo sucesivo, C.p.) en cuando a los delitos contra la libertad sexual para luchar contra los abusos sexuales, la explotación sexual de menores y la pornografía infantil, elevándose la edad para consentir válidamente relaciones sexuales de los 13 a los 16 años.

Ante este escenario normativo tan variopinto (ciertamente, es para volverse loco) y sólo cuando esté suficientemente justificada la mayoría de edad para prestar consentimiento, creemos que la edad para consentir la cesión de datos personales es 14 años y tanto para el ámbito sanitario como para el bioinvestigador debería ser la misma, 16 años. Ello respondería al máximo respeto del menor maduro y de sus deseos vitales, así como a la autonomía real que hoy, sin lugar a dudas, tiene el adolescente.

Propuesto *de lege ferenda* lo anterior, la LIB genera muchas dudas en la práctica que deja sin resolver, razón por la cual lo único que nos queda es acudir al articulado del C.c, el cual parte, en su art. 162, de que el menor maduro tiene capacidad para ejercer por sí solo sus derechos de la personalidad.

De este modo, en caso de discrepancia entre los titulares de la patria potestad a la hora de prestar el consentimiento, por representación, de su hijo menor de edad para la cesión de sus muestras con fines de investigación, debemos recurrir a las reglas de ejercicio de la patria potestad contenidas en el art. 156 C.c.[44]. Si bien es cierto que dicho precepto arroja cierta luz, son muchas las dudas que deja en el aire, entre otras: ¿es posible que un padre conceda al otro un consentimiento general para el ejercicio de todas las facultades inherentes a la patria potestad?; ¿qué sucede cuando uno de

[44] Para un análisis detenido de dicho precepto, *vid*. Castán Vázquez, J. Mª., "Comentario al art. 156", *Comentario del Código civil*, Tomo I, Ed. Ministerio de Justicia, Madrid, España, 1993, pp. 550-553.

los progenitores realiza un acto sin el consentimiento del otro fuera de los supuestos de actuación unilateral previstos por la ley?; ¿cómo se acredita el ejercicio exclusivo del ejercicio de la patria potestad?; ¿cómo se ejerce la patria potestad en caso de ruptura parental contenciosa, pero aún sin judicializar y, por consiguiente, sin medidas provisionales sobre los hijos? Pese a ello, de gran importancia práctica para el profesional sanitario o investigador es lo dispuesto por el art. 156 C.c. en su párrafo 3º: "en los supuestos de los párrafos anteriores, respecto de terceros de buena fe, se presumirá que cada uno de los progenitores actúa en el ejercicio ordinario de la patria potestad con el consentimiento del otro".

Si se trata de un supuesto de separación o divorcio, habrá que estarse a lo que indique la sentencia y, en concreto, al régimen de guarda (individual o compartida) y al tipo de decisión que haya de tomarse.

¿Cómo ha de resolverse un conflicto entre un menor de edad con madurez volitiva suficiente y sus representantes legales? ¿quién ha de decidir la voluntad que debe prevalecer? Creemos que, inicialmente, el profesional y, en caso de duda o de que la decisión de los representantes legales sea perjudicial para el menor, habrá de recurrirse a la autoridad judicial, conforme a lo dispuesto por los arts. 158.4 y 216 C.c. En este último caso, el juez deberá decidir, ponderadamente, entre la tutela del interés superior del menor y la del derecho a la investigación científica.

En caso de consentimiento por los representantes legales con opinión contraria del menor y perjuicio a éste, ¿podría éste, con posterioridad, ejercitar una acción de responsabilidad por actuación ilegítima de sus representantes legales *ex* art. 1902 C.c.?

¿*Quid iuris* si el padre o madre del sujeto fuente menor de edad también lo es? Pues el art. 157 C.c. dispone que "el menor no emancipado ejercerá la patria potestad sobre sus hijos con la asistencia de sus padres y, a falta de ambos, de su tutor; en casos de desacuerdo o imposibilidad, con la del Juez".

Otra duda a despejar: si el menor tiene suficiente grado de discernimiento y, en todo caso, según mantenemos, a partir de los 16 años, a quién han de comunicarse los resultados de la investigación, ¿a él de manera individualizada, a sus representantes legales o a ambos? Creemos que lo más respetuoso con los derechos fundamentales del menor de edad con capacidad de juicio y entendimiento suficiente es comunicarle sólo a él los resultados.

Cuestión de interés en el ámbito de la investigación biomédica e irresuelta también por el legislador gira en torno a si al llegar a la mayoría de edad es o no preciso recontactar con el sujeto fuente de la muestra biológica para refrendar o, en cambio, si así lo desea, ejercer su derecho de revocación del consentimiento informado que, en su lugar, prestaron sus representantes legales. Dos son las posturas: de un lado, debe recontactarse con el menor al cumplir 18 años; de otro, no es preciso pues es responsabilidad de los representantes legales mantener informados a sus hijos.

Nos decantamos por la primera, pues, además de ser lo más respetuoso con los derechos de la persona y considerar que el consentimiento no es estático o de tracto único, ya la propia LIB lo contempla para la persona se encuentra en situación de incapacidad para consentir debido a su situación clínica, a quien "se deberá solicitar el consentimiento para continuar participando en las investigaciones, en cuanto el paciente se halle en condiciones de prestarlo" (art. 21.4 LIB). Por otra parte, como ya vimos, el art. 23.2.n) del RD 2011 contempla que el documento de consentimiento para la obtención, almacenamiento o conservación y utilización de muestras biológicas de origen humano con fines de investigación biomédica contenga, en el caso de almacenamiento de muestras de menores de edad, "garantía de acceso a la información indicada en el artículo 32 sobre la muestra por el sujeto fuente cuando éste alcance la mayoría de edad". Y, por último, el art. 4.3 del RD 1090/2015, de ensayos clínicos con medicamentos, dispone que cuando el menor o persona con capacidad modificada alcance o recupere la capacidad de consentir, deberá recabarse su consentimiento para continuar participando en el ensayo clínico, fórmula legal que nos parece muy acertada. Siendo ésta la norma más reciente de todas en este ámbito, nos preguntamos si dicha previsión normativa marca la pauta a seguir o, en cambio, se ciñe únicamente a los ensayos clínicos sin que pueda extrapolarse a la investigación biomédica.

Sorprende cómo en materia de menores de edad, cuyos derechos e intereses deben ser especialmente protegidos por los órganos jurisdiccionales y por el Ministerio Fiscal, la LIB contempla exclusivamente la intervención de éste en el supuesto de que la investigación no vaya a producir beneficios directos para los sujetos, en cuyo caso la Ley dispone que la autorización de la investigación deba ponerse en conocimiento del Ministerio Fiscal (art. 20.2.c LIB). Al respecto, ha de destacarse que no es lo mismo poner en conocimiento del Ministerio Fiscal que solicitar autorización con carácter previo a la obtención de la muestra, lo cual supondría mayores garantías para los derechos del sujeto fuente menor de edad.

Creemos que debería darse mayor protagonismo al Ministerio Fiscal mediante fórmulas operativas en la práctica, como la puesta en conocimiento, con carácter previo, de una decisión relativa a un menor de edad y, en caso de su falta de respuesta en un plazo prudencial, se entendería su anuencia, al estilo de lo contemplado por el art. 3.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Una última cuestión de enorme interés práctico: el acceso o no a los datos de la historia clínica del hijo menor de edad mayor de 14 años (en la que se fija la capacidad para consentir por sí solo el tratamiento de sus datos personales) o, en su caso, de 16 (mayoría de edad sanitaria, esto es, capacidad para consentir el acto médico) por parte de sus representantes legales.

Si bien la Agencia Española de Protección de Datos, en su Informe 409/2004, contemplaba la necesidad de que el mayor de 14 años no incapacitado judicialmente autorizara, de forma fehaciente, a su padre o madre para acceder a su historia clínica, diez años después, en su Informe 0222/2014, considera que los titulares de la patria potestad pueden acceder a los datos del hijo menor sujeto a aquélla durante toda su minoría de edad para poder cumplir las obligaciones previstas en el art. 154 C.c. De este modo, estando obligados los titulares de la patria potestad a cumplir las funciones y deberes impuestos en virtud del sistema de guarda que ostentan, entre ellos, velar por el menor, no sería oponible al acceso a la historia clínica la mera voluntad del menor sometido a patria potestad, con la única excepción de que una norma con rango de Ley hiciese expresamente primar la voluntad del menor sobre la de los titulares que pretenden el acceso.

Pensamos que dicho cambio de opinión experimentado por la Agencia Española de Protección de Datos tal vez pueda ser debido a que ha de tenerse en cuenta que, además de la responsabilidad parental que ostentan los progenitores (y, en su caso, el tutor), éstos también son responsables civilmente por los ilícitos cometidos por el menor *ex* art. 1903 C.c., por ello que tengan derecho a conocer sus datos clínicos (p. ej. consumo de drogas, padecimiento de enfermedades de transmisión sexual como el VIH, etc.). En todo caso, habrá que estarse al caso concreto (tipo de información, edad del menor, finalidad, intereses en juego, etc.) y guiarse por el por el interés superior del menor[45].

[45] De esta opinión, Andreu Martínez, Mª. B., *La autonomía del menor en la asistencia sanitaria y el acceso a la historia clínica*, *op. cit*., pp. 95-96.

En conclusión, creemos que el menor maduro debe gozar de un *status quo* claro, ajeno a los cambios legislativos y con un marco normativo interno menos proteccionista o paternalista como lo es el actual y más humano o existencial.

4.2. El derecho a la accesibilidad universal de la persona con discapacidad

En 2018 hemos conmemorado el décimo aniversario de la entrada en vigor en el ordenamiento jurídico español de la Convención ONU de los derechos de las personas con discapacidad, Tratado internacional que ha sido crucial en materia de derechos humanos por su enorme impacto, marcando un antes y un después en la evolución de los derechos de las personas diversamente capaces (repárese en la expresión utilizada, en positivo y plural).

Su aplicación ha supuesto avances importantísimos, destacadamente, la visibilización de las personas con discapacidad (con independencia del tipo de deficiencia y de si tienen o no modificada su capacidad) poniendo el acento en la persona y no en su deficiencia, pero es igualmente cierto que aún faltan muchos retos por alcanzar en su interpretación, grado de cumplimiento y desarrollo normativo.

Dicho Instrumento ha conllevado, sin lugar a dudas, un cambio paradigmático de actitud y enfoque respecto de la discapacidad a nivel mundial[46]. Se mira la discapacidad con otros ojos. La Convención advierte a España (que la ratificó en 2008) y a los restantes Estados así como a las Organizaciones supranacionales (como la Unión Europea[47]) firmantes que el único abordaje que puede hacerse de la discapacidad es desde los derechos humanos y libertades fundamentales de la persona[48].

---

[46] En el ámbito de la discapacidad, se percibe, claramente, la reciente "humanización" que están experimentando los legisladores internacionales, europeos y nacionales, como señalábamos en Vivas-Tesón, I., "Retos actuales en la protección jurídica de la discapacidad", *Revista Pensar*, Núm. 3, Vol. 20, 2015, p. 825. Disponible en: http://periodicos.unifor.br/rpen/article/view/4110 [Última consulta: 30 de agosto de 2019].

[47] La Unión Europea ratificó la Convención en el año 2011, siendo la primera vez que dicha organización supranacional llega a ser parte de un Tratado internacional.

[48] Así lo subrayamos en nuestro trabajo Vivas-Tesón, I., *Más allá de la capacidad de entender y querer***.** *Un análisis de la figura italiana de la administración de apoyo y una propuesta de reforma del sistema tuitivo español,* Ed. Futuex, Olivenza, Badajoz, España, 2012, pp. 20 y ss.

Para la Convención es necesario poner todos los medios posibles con el fin de conocer la voluntad, deseos y preferencias de la persona con discapacidad[49] [50].

Los cambios para adaptar nuestro ordenamiento jurídico a los principios, valores y mandatos de tan importante Tratado internacional han comenzado por algo tan simple y a la vez tan potente como es la utilización de un lenguaje adecuado y respetuoso. Las palabras demuestran cultura, el grado de civilización, el modo de pensar, respeto. No se trata de un mero lenguaje políticamente correcto. No es algo banal. Cambiemos el lenguaje y cambiaremos el mundo.

Ahora hablamos de "personas con discapacidad"[51]. Como puede comprobarse, el foco de atención se centra en la persona y no en su condición, la

[49] En este sentido, la Sentencia del Tribunal Supremo (Sala de lo civil, Sección 1ª) de 30 de septiembre de 2014 señala: "puede subrayarse la improcedencia de desconocer la voluntad de la persona discapacitada. Es cierto que en determinados casos esta voluntad puede estar anulada hasta el extremo de que la persona discapacitada manifieste algo que objetivamente la perjudique. Pero esta conclusión sobre el perjuicio objetivo debe ser el resultado de un estudio muy riguroso sobre lo manifestado por la persona discapacitada y sus consecuencias a fin de evitar que lo dicho por ella se valore automáticamente como perjudicial, y lo contrario, como beneficioso". Y continúa: "a tenor de lo establecido en la Convención sobre los Derechos de las Personas con Discapacidad, la voluntad de la persona discapacitada (en el caso, incapacitada por decisión judicial) debe ser respetada salvo que razones objetivas permitan concluir que ello la perjudicaría".

[50] Como expresa el Alto tribunal (Sala de lo civil, Sección 1ª) en su Sentencia de 16 de mayo de 2017, la Convención "opta por un modelo de apoyos para configurar el sistema dirigido a hacer efectivos los derechos de las personas con discapacidad (art. 12.3). Se trata, como declara el art. 1 de la Convención, de promover, proteger y asegurar el goce pleno y en condiciones de igualdad de todos los derechos humanos y libertades fundamentales por todas las personas con discapacidad y promover el respeto de su dignidad inherente. Con el fin de hacer efectivo este objetivo, los Estados deben asegurar que en todas las medidas relativas al ejercicio de la capacidad se proporcionen salvaguardias adecuadas y efectivas para impedir los abusos. Esas salvaguardias deben asegurar que las medidas relativas al ejercicio de la capacidad respeten los derechos, la voluntad y las preferencias de la persona, que no haya conflicto de intereses ni influencia indebida, que sean proporcionales y adaptadas a las circunstancias de la persona. En particular, las salvaguardias, deben ser proporcionales al grado en que dichas medidas afecten a los derechos e intereses de las personas (art. 12.4 de la Convención). Desde esta perspectiva debe interpretarse lo dispuesto en el C.c y en la Ley de Enjuiciamiento civil..." (FJ. 5º).

[51] Si bien el legislador español ya utilizó dicha nomenclatura en la Ley 41/2003, de 18 de noviembre, que lleva por rúbrica "Protección patrimonial de las personas con discapacidad" (no "discapacitadas"), sería en la Disposición Adicional 8ª de la Ley 39/2006, de 14 de diciembre de 2006, de Promoción de la Autonomía Personal y Atención a las personas en situación de Dependencia, en la que dispusiera que las referencias contenidas en los textos normativos a los "minusválidos" y a las "personas con minusvalía", se debían entender realizadas a "personas con discapacidad" (si se nos permite el símil, como en el procesador de texto la utilización de "buscar" y "reemplazar"), y que dicho término

cual viene después y con carácter accesorio. Conforme a ello, discapacitado como sustantivo no debe utilizarse, pues confunde una parte con el todo. Somos muy dados a etiquetar, a encasillar, a clasificar.

Centrándonos en la materia objeto de nuestras reflexiones, tanto el RD 1090/2015 de ensayos clínicos como la LOPDyGDD, de fecha posterior a la ratificación de la Convención por parte de España, acogen dicha terminología; la LAP ha sido retocada a tal efecto en el año 2011 y, curiosamente, la LIB no, puesto que, aun siendo anterior a la ratificación del Tratado, ya la incorporaba en su texto normativo.

Pese a las mejoras y avances en materia de derechos humanos y discapacidad, aún quedan algunas piezas del puzle sin encajar e importantes retos por cumplir.

A nuestro entender, en Derecho español existe una clara disfunción o desajuste a resolver lo antes posible, pues la imprescindible exigencia normativa de un reconocimiento formal de discapacidad con un grado mínimo del 33% no casa adecuadamente con la definición de discapacidad contenida en el art. 1, pfo. 2º de la Convención[52], de modo que la discapacidad no se presenta por deficiencias concretas de las personas, sino por diversas barreras que pueden ser sociales, físicas, actitudinales o jurídicas, lo que permite establecer como objetivo la eliminación de las barreras existentes de toda índole) y, por tanto, creemos que no se ajusta al modelo social de la misma como sí, en cambio, el art. 2.a) del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad[53] y

---

sería el utilizado para denominarlas en las disposiciones normativas elaboradas por las Administraciones Públicas.
Sorprendentemente, el art. 49 de la Constitución Española de 1978 sigue aún conservando, el término "disminuidos": "los poderes públicos realizarán una política de previsión, tratamiento, rehabilitación e integración de los disminuidos físicos, sensoriales y psíquicos, a los que prestarán la atención especializada que requieran y los ampararán especialmente para el disfrute de los derechos que este Título otorga a todos los ciudadanos", si bien el Consejo de Ministros aprobó en diciembre de 2018 un Anteproyecto de reforma constitucional para eliminar dicha palabra.

52 "Las personas con discapacidad incluyen a aquellas que tengan deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás".

53 Art. 2: "A efectos de esta ley se entiende por: a) Discapacidad: es una situación que resulta de la interacción entre las personas con deficiencias previsiblemente permanentes y cualquier tipo de barreras que limiten o impidan su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás".

de su inclusión social, así como el art. 25 del C.p. en su redacción de 2015[54]. Para mayor confusión, dicho certificado administrativo sigue exigiéndose para algunos actos jurídicos, pero no, en cambio, para otros, como, por ejemplo, en la Ley de Propiedad Horizontal, que en su art. 10.1.b) reconoce automáticamente a los mayores de 70 años su condición de personas con discapacidad. A la vista de ello, nos preguntamos: hoy día, en el ordenamiento español, ¿quién es, desde el punto de vista jurídico, una persona con discapacidad?

Por otra parte, las diversas lecturas que del texto internacional hemos realizado a lo largo de estos diez años nos han conducido siempre a extraer la conclusión (la cual, incluso, he tenido ocasión de dejar reflejada por escrito) de que la Convención de Nueva York no reconocía ningún derecho nuevo que no estuviera ya contenido en anteriores Tratados internacionales. Sin embargo, hoy por hoy, discrepamos, pues estamos plenamente convencidos de que sí reconoce, con contundencia, un nuevo derecho: el derecho a la accesibilidad universal (no sólo arquitectónica, en la cual solemos únicamente pensar), esto es, al ejercicio accesible y efectivo de todos los derechos para tener una vida plena e independiente, incluido el derecho a elegir su recorrido vital y el derecho a equivocarse.

Sólo así se da cumplimiento no sólo a lo dispuesto a la célebre "estrella polar" de la Convención, su art. 12, sino, junto a éste, otro precepto que, a nuestro juicio, es igualmente crucial y por ello no tiene sentido uno sin el otro, el 19 y su reconocimiento al derecho a una vida independiente e inclusiva en la comunidad. Se trata ésta de una disposición normativa transversal y, por ello, íntimamente interrelacionada con las restantes contenidas en el Tratado de Nueva York, pese a lo cual, extrañamente, no suele prestársele tanta atención como al art. 12.

El citado art. 19 se basa en el principio fundamental de derechos humanos de que todos los seres humanos nacen iguales en dignidad y en derechos y todas las vidas tienen el mismo valor, como señala la Observación general núm. 5 (2017) del Comité sobre los Derechos de las personas con discapacidad sobre el derecho a vivir de forma independiente y a ser incluido en la comunidad[55], la cual enfatiza dicho derecho tanto en su dimensión

[54] Art. 25: "A los efectos de este Código se considera incapaz a toda persona, haya sido o no declarada su incapacitación, que padezca una enfermedad de carácter persistente que le impida gobernar su persona o bienes por sí misma".

[55] Disponible en: http://www.ohchr.org/EN/HRBodies/CRPD/Pages/CRPDIndex.aspx [Última consulta: 30 de agosto de 2019].

individual[56] como social de plena inclusión y participación en aquélla[57]. El derecho consagrado en el art. 19 de la Convención, como señala la citada Observación general nº 5, abarca ambas dimensiones.

Así las cosas, los arts. 12 y 19 están directamente conectados o vinculados porque el reconocimiento de la personalidad y capacidad jurídicas es la base para que la ciudadanía con discapacidad logre vivir, de forma independiente y plena, en el seno de la comunidad. Por consiguiente, es preciso garantizar a todas las personas con discapacidad, con independencia de su concreta deficiencia, el derecho a la capacidad jurídica (de goce y de ejercicio), para decidir dónde, cómo y con quién vivir.

---

[56] Para la citada Observación general nº 5, vida independiente significa "que las personas con discapacidad cuenten con todos los medios necesarios para que puedan tomar opciones y ejercer el control sobre sus vidas, y adoptar todas las decisiones que las afecten. La autonomía personal y la libre determinación son fundamentales para la vida independiente, incluidos el acceso al transporte, la información, la comunicación y la asistencia personal, el lugar de residencia, la rutina diaria, los hábitos, el empleo digno, las relaciones personales, la ropa, la nutrición, la higiene y la atención de la salud, las actividades religiosas y culturales, y los derechos sexuales y reproductivos. Las siguientes actividades están vinculadas al desarrollo de la identidad y la personalidad de cada individuo: dónde vivimos y con quién, qué comemos, si nos gusta dormir hasta tarde o acostarnos a altas horas de la noche, si preferimos quedarnos en casa o salir, si nos gusta poner mantel y velas en la mesa, tener animales domésticos o escuchar música. Tales acciones y decisiones nos hacen ser quienes somos. La vida independiente es una parte esencial de la autonomía y la libertad de la persona y no significa necesariamente vivir solo. Tampoco debe interpretarse únicamente como la capacidad de llevar a cabo actividades cotidianas por uno mismo. Por el contrario, debe considerarse como la libertad de elección y de control, en consonancia con el respeto de la dignidad inherente y la autonomía individual consagradas en el artículo 3 a) de la Convención. La independencia como forma de autonomía personal implica que la persona con discapacidad no se vea privada de la posibilidad de elegir y controlar su modo de vida y sus actividades cotidianas".
Por tanto, como puede comprobarse, las decisiones personales abarcan todos los aspectos del sistema de vida de la persona tanto en la esfera privada como en la pública y tanto en lo cotidiano como a largo plazo.

[57] Según la Observación general nº 5, "el derecho a ser incluido en la comunidad se refiere al principio de inclusión y participación plenas y efectivas en la sociedad consagrado, entre otros, en el artículo 3 c) de la Convención. Incluye llevar una vida social plena y tener acceso a todos los servicios que se ofrecen al público, así como a los servicios de apoyo proporcionados a las personas con discapacidad para que puedan ser incluidas y participar plenamente en todos los ámbitos de la vida social. Esos servicios pueden referirse, entre otras cosas, a la vivienda, el transporte, las compras, la educación, el empleo, las actividades recreativas y todas las demás instalaciones y servicios ofrecidos al público, incluidos los medios de comunicación social. Ese derecho también incluye tener acceso a todas las medidas y acontecimientos de la vida política y cultural de la comunidad, entre otras cosas reuniones públicas, eventos deportivos, festividades culturales y religiosos y cualquier otra actividad en la que la persona con discapacidad desee participar".

En nuestra modesta opinión, la accesibilidad se erige como un nuevo derecho de la personalidad. La no accesibilidad a los derechos es una flagrante violación de la dignidad humana, puesto que si los derechos reconocidos a todas las personas sin excepción no pueden disfrutarse plena y efectivamente no puede vivirse una vida digna[58].

Esto dicho, por accesibilidad no ha de entenderse sólo la física o arquitectónica, sino la universal, en la que se comprende, además, la sensorial y la cognitiva. En relación a esta última, concerniente a la supresión de barreras de compresión y comunicación, creemos necesario que en toda norma en la que se regule el consentimiento informado para un determinado acto se contemple que tanto la información previa como el proceso de prestación del consentimiento sean no sólo accesibles, sino también comprensibles.

Una buena fórmula legal que consideramos extrapolable a otras materias (por ejemplo, cesión de datos de carácter personal, en cuya LOPDyGDD, lamentablemente, brilla por su ausencia) nos parece el art. 9.5º de la LAP, en su redacción dada por la de la Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención ONU[59]. Como puede comprobarse, en dicho tenor literal se contiene la obligación de prestar medidas de apoyo necesarias, haciéndose hincapié no sólo en la accesibilidad física sino también en la cognitiva, crucial en una materia repleta de tecnicismos.

Nos resulta curioso que la citada Ley 26/2011 modificara también el art. 10 de la Ley 14/1986, de 25 de abril, General de Sanidad aunque no con idéntica redacción[60], pasando por alto el art. 4.1, pfo. 3º de la Ley 14/2007, de 3 de julio, de Investigación biomédica, el cual sigue manteniendo intacta su redacción originaria por la que establece que la información que ha de proporcionarse a las personas con discapacidad con carácter previo al consentimiento se les prestará "en condiciones y formatos accesibles apropiados

[58] Vivas-Tesón, I., "El ejercicio de los derechos de la personalidad de la persona con discapacidad", De Salas Murillo, S. / Mayor del Hoyo, Mª. V. (Dirs.), *Claves para la adaptación del ordenamiento jurídico privado a la Convención de Naciones Unidas en materia de discapacidad*, Ed. Tirant lo Blanch, Valencia, España, 2019, p. 412.

[59] "…Si el paciente es una persona con discapacidad, se le ofrecerán las medidas de apoyo pertinentes, incluida la información en formatos adecuados, siguiendo las reglas marcadas por el principio del diseño para todos de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que pueda prestar por sí su consentimiento".

[60] "Todos tienen los siguientes derechos con respecto a las distintas Administraciones públicas sanitarias: 2. (...) La información deberá efectuarse en formatos adecuados, siguiendo las reglas marcadas por el principio de diseño para todos, de manera que resulten accesibles y comprensibles a las personas con discapacidad".

a sus necesidades". Creemos que se ha perdido una magnífica oportunidad para adaptar la LIB a la Convención de Nueva York.

Así las cosas, en relación a las personas con discapacidad, consideramos importante recalcar las siguientes ideas: que tienen plena capacidad jurídica salvo que un órgano judicial se la modifique; que es necesario eliminar todo tipo de barreras y obstáculos que impiden su inclusión en la sociedad[61] como ciudadanos de pleno derecho; y que requieren acompañamiento o apoyo, no sustitución en la toma de decisiones.

4.3. La persona con capacidad judicialmente modificada. Un breve apunte del Anteproyecto de ley de reforma de la legislación civil y procesal en materia de discapacidad

Para comenzar, debemos distinguir entre persona en situación de incapacidad de hecho (lo que la LIB denomina en su art. 21 "en situaciones clínicas de emergencia en las que la persona implicada no pueda prestar su consentimiento" y el art. 7 del RD 1090/2015 de ensayos clínicos, "en situaciones de urgencia", preceptos a los cuales nos remitimos, no sin advertir la importancia en estos supuestos de los poderes preventivos) y persona con capacidad judicialmente modificada (mejor que "incapacitada judicialmente", nomenclatura que aún conserva la LIB), en cuyo caso hay que estar únicamente a lo indicado expresamente en la sentencia judicial (y no a las afirmaciones de familiares o allegados), la cual debe ser un traje a medida y no, por tanto, *prêt-à-porter*. Por consiguiente, el profesional sanitario o investigador debe, sencillamente, solicitar la sentencia judicial y comprobar en ella si la persona puede o no prestar su consentimiento por sí sola. También ha de tener muy en cuenta que dicha situación no es irreversible, por ello que la sentencia sea revisable, lo que obliga a estar al último pronunciamiento judicial dictado al respecto.

[61] Como señala el Informe "Estado mundial de la Infancia 2013: niños y niñas con discapacidad" de UNICEF, "la inclusión va más allá de la integración. Por ejemplo, en la esfera educativa, la integración significaría, sencillamente, admitir a los niños y niñas con discapacidad en las escuelas 'generales'. La inclusión, sin embargo, solo es posible cuando el diseño y la administración de las escuelas permiten que todos los niños y las niñas participen juntos de una educación de calidad y de las oportunidades de recreación. Esto supondría proporcionar a los estudiantes con discapacidad facilidades como acceso al sistema braille y al lenguaje de señas, y adaptar los planes de estudios". Disponible en: https://www.unicef.org/spanish/sowc2013/files/SPANISH-SOWC13-Ex_Summary_Lores_web.pdf [Última consulta: 30 de agosto de 2019].

Al respecto, nos parece todo un acierto (aunque la redacción es mejorable) la modificación operada en 2015 en el art. 9.3.b) de la LAP: "3. Se otorgará el consentimiento por representación en los siguientes supuestos: b) Cuando el paciente tenga la capacidad modificada judicialmente y así conste en la sentencia". De este modo, se pone todo el acento en la sentencia, en la cual debe constar que la persona tiene su capacidad modificada para el acto de prestación del consentimiento en el ámbito sanitario y, por tanto, debe ser otorgado por representación. Si nada se indicara al respecto, la persona tiene plena capacidad para prestarlo por sí sola.

Si bien es frecuente encontrar que en las sentencias se mencione el consentimiento a tratamientos sanitarios, difícilmente un juez va a reparar en el consentimiento para cesión de muestras con fines de investigación, como parece plantear, de manera un tanto utópica, el art. 20.1 LIB: "la investigación sobre una persona menor o incapacidad de obrar, salvo que, en atención a su grado de discernimiento, la resolución judicial de incapacitación le autorizase para prestar su consentimiento a la investigación (...)".

Por otra parte, el art. 4.2 LIB dispone que "las personas incapacitadas… participarán en la medida de lo posible y según su edad y capacidades en la toma de decisiones a lo largo del proceso de investigación". En la práctica, ¿se les brinda, realmente, la oportunidad de participar en dicho proceso?

El RD 2011 omite por completo el tratamiento de las muestras biológicas procedentes de personas con capacidad judicialmente modificada, teniéndose en cuenta, exclusivamente, a los menores de edad en cuanto a la garantía para el acceso de la información cuando alcancen la mayoría de edad (arts. 23.n y 32.3). ¿Significa ello que las personas con capacidad de obrar modificada judicialmente que posteriormente la recuperen no tienen reconocida tal garantía? Creemos que no y que ello es debido a un lamentable olvido que debiera subsanarse cuanto antes.

El RD 1090/2015 de ensayos clínicos, si bien acoge la terminología de "persona con capacidad modificada", olvida por completo la necesidad de acudir a lo dispuesto judicialmente en la sentencia y, en su art. 6.3, indica directamente que es necesario obtener el consentimiento informado previo del representante legal. Sin embargo, es curioso que dicha norma contemple acertadamente en su art. 4.3 que cuando la persona con capacidad modificada alcance o recupere la capacidad de consentir, deberá recabarse su consentimiento para continuar participando en el ensayo clínico.

Visto lo anterior, todo ello podría cambiar próximamente y, además, de manera radical.

Tras diez años de larga espera, parece que, por fin, ha llegado el momento de afrontar la reforma de la legislación civil y procesal en materia de discapacidad. En septiembre de 2018 el Consejo de Ministros aprobó el Anteproyecto de Ley por la que se acometerá dicha reforma[62], la cual, con mejoras técnicas en su texto, confiamos en que muy pronto pueda ver la luz cuando lo retome el nuevo Gobierno.

Haciendo un brevísimo comentario acerca de dicha iniciativa legislativa, ésta sintoniza claramente con la Convención de Nueva York y con su enfoque de derechos humanos al pretenderse, a toda costa, indagar la voluntad, deseos y preferencias de la persona con discapacidad[63], quedando relegado su interés[64], como afirma en su Exposición de Motivos[65].

---

[62] Los textos que pretende reformar son el Código civil, la Ley de Enjuiciamiento civil, la Ley Hipotecaria y la Ley del Registro civil.

[63] Para Pau Pedrón, "este es un punto de gran relevancia, en torno al cual gira el cambio profundo que se lleva a cabo en materia de discapacidad: el "interés de la persona con discapacidad" hay que situarlo detrás de "la voluntad, deseos y preferencias de la persona". El "interés de la persona con discapacidad" no aparece nombrado en ningún momento a lo largo de la Propuesta, a diferencia del concepto de "interés del menor", que aparece nueve veces citado en el Código civil. Lo mismo sucede en la Convención de 2006: en ningún momento se habla del "interés de la persona con discapacidad", mientras que el "interés del niño" aparece mencionado tres veces". Pau Pedrón, A., "De la incapacitación al apoyo: el nuevo régimen de la discapacidad intelectual en el Código civil", *Revista de Derecho civil*, Núm. 3, Vol. 5, Julio-Septiembre 2018, p. 8.

[64] Como señala Pau Pedrón, "cuando esa `voluntad, deseos y preferencias´ de la persona con discapacidad no están plenamente formadas, es necesario contribuir a esa formación. Hay que procurar que la persona con discapacidad tenga, efectivamente, una determinada `voluntad, deseos y preferencias´". Por eso dice el artículo 248 de la Propuesta que "las personas que presten apoyo […] procurarán que la persona con discapacidad pueda desarrollar su propio proceso de toma de decisiones, informándola, ayudándola en su comprensión y razonamiento y facilitando que pueda expresar sus preferencias". Conforme a ello, el Presidente de la Sección Primera, de Derecho civil, de la Comisión general de Codificación, indica que "el `interés de la persona con discapacidad´ queda muy relegado en relación con la voluntad de la persona –y situado incluso detrás la voluntad presunta–", por ello que, a su juicio no acierten algunos ordenamientos en poner en primer plano el interés, como el Código civil catalán (art. 221-1), el ABGB austriaco (§ 275, ap. 1) o el Código civil francés (art. 415). Y concluye: "Por tanto, en la contraposición de los criterios del `interés´ y la `voluntad´, hay que hay que dar preferencia a esta última. Sólo cuando la voluntad no puede expresarse ni reconstruirse, entrará el juego el criterio del interés". Pau Pedrón, A., "De la incapacitación al apoyo: el nuevo régimen de la discapacidad intelectual en el Código civil", *op. cit*., p. 9.

[65] "La nueva regulación está inspirada, como nuestra Constitución en su artículo 10 exige, en el respeto a la dignidad de la persona, en la tutela de sus derechos fundamentales

La idea central del nuevo sistema es la de apoyo a la persona que lo precise para el ejercicio de su capacidad jurídica (se destierra de nuestro ordenamiento la clásica dicotomía capacidad jurídica/capacidad de obrar) tanto para los asuntos personales como para los patrimoniales.

Tales apoyos para el ejercicio de la capacidad jurídica pueden ser voluntarios (poderes y mandatos preventivos así como la autocuratela) y judiciales (la guarda de hecho –la cual se transforma en una institución jurídica de apoyo que podría ser autorizada judicialmente para representar a la persona–, el defensor judicial –quien pasará también a complementar la capacidad del menor emancipado– y la curatela –meramente asistencial o bien con facultades representativas–, eliminándose del ámbito de la discapacidad no sólo la tutela, sino también la patria potestad (prorrogada o rehabilitada), que, según la propuesta, quedan reservadas como figuras de representación legal para el menor de edad. Todo ello merece nuestra valoración positiva, si bien echamos en falta un instrumento de apoyo voluntario similar a la figura de la asistencia catalana[66] para aquellos supuestos de disminución no incapacitante de las facultades físicas o psíquicas de la persona.

En cuanto a los aspectos procesales, el procedimiento de incapacitación judicial, que ha pasado a denominarse de modificación de la capacidad, vuelve a cambiar de nombre en la propuesta: "procedimiento de provisión de apoyos", el cual se diseña como "un sistema de colaboración interprofesional o 'de mesa redonda', con profesionales especializados de los ámbitos jurídico, asistencial y sanitario, que aconsejen las medidas de apoyo que resulten idóneas en cada caso", según recoge la Exposición de Motivos del citado Anteproyecto de ley.

5. Bibliografía

AA.VV., *Menores e investigación biomédica*, Gómez Sánchez, Y. (Coord.), Ed. Dykinson, Madrid, España, 2018.

---

y en el respeto a la libre voluntad de la persona con discapacidad, así como a los principios de necesidad y proporcionalidad de las medidas de apoyo que, en su caso, pueda necesitar esa persona para el ejercicio de su capacidad jurídica en igualdad de condiciones con los demás. Al respecto, ha de tomarse en consideración que, como ha puesto en evidencia la Observación General del Comité de Expertos de las Naciones Unidas elaborada en 2014, dicha capacidad jurídica abarca tanto la titularidad de los derechos, como la legitimación para ejercitarlos".

[66] Arts. 226-1 a 226-7 del Código civil de Cataluña.

Andreu Martínez, Mª. B., *La autonomía del menor en la asistencia sanitaria y el acceso a la historia clínica*, Ed. Aranzadi, Cizur Menor, Navarra, España, 2018.

Bosisio, R., "La percezione dei diritti nell'infanzia e nell'adolescenza. Una ricerca empirica", *Sociologia del Diritto*, Núm. 1, 2005.

Castán Vázquez, J. Mª., "Comentario al art. 156", *Comentario del Código civil*, Tomo I, Ed. Ministerio de Justicia, Madrid, España, 1993.

Chieffi, L., "La tutela della riservatezza dei dati sensibili: le nuove frontiere europee", *federalismi.it*., Núm. 4, 2018.

De Montalvo Jääskeläinen, F., *Menores de edad y consentimiento informado*, Ed. Tirant lo Blanch, Valencia, España, 2019.

Guilarte Martín-Calero, C., "El interés superior del niño: la nueva configuración del artículo 2 de la Ley Orgánica, de 15 de enero, de protección jurídica del menor", Cabedo Mallol, V. J. / Ravetllat Ballesté, I. (Coords.), *Comentarios sobre las Leyes de reforma del sistema de protección a la infancia y la adolescencia*, Ed. Tirant lo Blanch, Valencia, España, 2016.

Hernández López, J. M., *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Ed. Aranzadi, Cizur Menor, Navarra, España, 2013.

Herrán Ortiz, A. I., "Aproximación al derecho a la protección de datos personales en Europa: el Reglamento general de protección de datos personales a debate", *Revista de Derecho, Empresa y Sociedad*, Núm. 8, 2016.

Nogueira Blanco, J., "Reglamento General de Protección de Datos (RGPD) y BIG DATA", *Actualidad Civil*, Núm. 5, 2018.

Palomar Olmeda, A. / Pérez González, C., *La protección de datos: su marco constitucional y el contexto del nuevo Reglamento.* Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre), 2008.

Pau Pedrón, A., "De la incapacitación al apoyo: el nuevo régimen de la discapacidad intelectual en el Código civil", *Revista de Derecho Civil*, Núm. 3, Vol. 5, Julio-Septiembre 2018.

Picontó Novales, Mª. T., "Derechos de la infancia: Nuevo contexto, nuevos retos", *Derechos y Libertades*, Núm. 21, 2009.

Quinn, P. / Liam, Q., "Big genetic data and its big data protection challenges", *Computer Law & Security Review*, Núm. 5, Vol. 34, Octubre 2018.

Romeo Casabona, C. Mª., "Implicaciones jurídicas de la utilización de muestras biológicas humanas y biobancos en investigación científica", 2007.

Troncoso Reigada, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Núm. 43, Julio-Diciembre 2012.

Villaverde Menéndez, I., "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal", *La protección de datos de carácter personal en los centros de trabajo*, Farriols i Solá, A. (Coord.), Ed. Cinca, Madrid, España, 2006.

Vivas-Tesón, I., *Más allá de la capacidad de entender y querer. Un análisis de la figura italiana de la administración de apoyo y una propuesta de reforma del sistema tuitivo español, Ed.* Futuex, O*livenza, Badajoz,* España*, 2012*.

Vivas-Tesón, I., "Retos actuales en la protección jurídica de la discapacidad", *Revista Pensar*, Núm. 3, Vol. 20, 2015.

Vivas-Tesón, I., "Uso y control de la información genética: dudas y retos para el Derecho privado", *Revista de Derecho Privado*, Núm. 5, Septiembre-Octubre 2016.

Vivas-Tesón, I., "El ejercicio de los derechos de la personalidad de la persona con discapacidad", De Salas Murillo, S. / Mayor del Hoyo, Mª. V. (Dirs.), *Claves para la adaptación del ordenamiento jurídico privado a la Convención de Naciones Unidas en materia de discapacidad*, Ed. Tirant lo Blanch, Valencia, España, 2019.

Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías *Bigdata*[*]

Regulation of data processing in health research projects, in particular in the application of Bigdata technologies

Profa. Dra. Itziar Alkorta Idiakez

Profesora Titular de Derecho Civil, Universidad del País Vasco UPV/EHU (San Sebastián, España)

DOI: 10.14679/1139

Sumario / Summary: 0. Introducción. 1. El marco normativo compuesto por el RGPD y la nueva LOPDGDD. 2. Principales novedades introducidas en el RGPD. 2.1. Enfoque basado en la protección de riesgos. 2.2. Evaluación de impacto. 2.3. Quiebras de seguridad y notificación. 3. Tratamiento de datos con tecnologías Bigdata. 3.1. Tratamiento masivo de datos o tratamiento de datos a gran escala. 3.2. Datos anonimizados y seudonimizados. 3.3. Adopción de medidas técnicas y organizativas. 3.4. Funciones encomendadas a las instancias encargadas de supervisar los proyectos de tratamientos Bigdata. 4. Utilización de datos personales con fines de investigación. 4.1. ¿Qué se entiende por "investigación científica"?. 4.2. La investigación como base legal específica para el tratamiento de datos personales. 4.3. El tratamiento

[*] Artículo recibido el 26 de febrero de 2019 y aceptado para su publicación el 5 de junio de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos -Big Data-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

posterior de los datos con fines de investigación. 4.4. Las garantías exigidas por el artículo 89 para el tratamiento de los datos dedicados a la investigación. 4.5. El deber de información y transparencia.4.6. Derecho de oposición. 4.7. La prohibición del perfilado a partir del uso secundario de datos para la investigación. 5. Marco legal para el uso de datos en investigación sanitaria y biomédica en la Ley Orgánica 3/2018. 5.1. Habilitación legal que salva el marco normativo vigente. 5.2. La regulación del consentimiento. 5.3. El consentimiento genérico. 5.4. Reutilización de datos de salud para la investigación biomédica.5.5. Investigación a partir de datos seudonimizados. 5.6. Garantías técnicas para los tratamientos de datos de salud en investigación. 5.7. Excepciones a los derechos ARCO. 5.8. Control ético de la investigación sanitaria. 6. Anexo. Ruta básica de control de los proyectos de investigación sanitaria y biomédica que impliquen tratamiento masivo de datos. 7. Bibliografía.

Resumen / Abstract: El presente trabajo tiene por finalidad aclarar el panorama dibujado por los nuevos instrumentos normativos europeos sobre protección de datos en orden a establecer unas rutas de control de los proyectos de investigación con datos de salud en entornos de Bigdata. Aclarar qué rutas debe seguir el investigador de la Biomedicina en el desarrollo de su su tarea sometiéndola a los nuevos controles éticos y jurídicos, contribuirá sin duda a mejorar la calidad de la investigación y de la protección del ciudadano, atendiendo también a un desempeño más eficiente de los órganos de decisión y autorización, que hoy se ven desbordados, no solo por las informaciones que deben tener en cuenta, sino por la constatación de la inseguridad que supone la interpretación de este nuevo marco normativo. Al mismo tiempo, este esfuerzo de clarificación pretende satisfacer la creciente y urgente demanda social de transparencia en la investigación biomédica.

This paper aims to clarify the picture drawn by new data protection regulatory instruments in order to establish control routes of health research projects in Bigdata environments. Clarifing which routes should follow the researcher in biomedicine in the development of their task by subjecting it to the new ethical and legal controls, will contribute to improve the quality of research and the protection of the citizen, also attending to a more efficient performance of decision making boards and control authorities. These instances are overwhelmed, not only for the information to be taken into account, but also because of the doubts posed by the interpretation of this new regulatory framework. At the same time, this effort is intended to meet the urgent and growing social demand for transparency in biomedical research.

Palabras clave / Keywords:

Datos de salud / BigData / Reglamento Europeo de Protección de Datos / Regulación española de protección de datos / Proyectos de investigación con datos.

Health data / BigData / General Data Protection Regulation / Spanish Regulation on Data Protection / Health Research wiht Data.

0. Introducción

La investigación sanitaria y la biomédica cuentan con una larga historia en relación a las exigencias éticas y normativas a las que se han sometido a lo largo del tiempo; en especial, a partir del Código de Núremberg de 1947.

En España, la evolución de este tipo de investigación científica ha conocido un desarrollo exponencial en los últimos decenios, hasta el punto de que destacados grupos de investigación han alcanzado cotas importantes de reconocimiento internacional. Por otra parte, el descubrimiento de nuevos fármacos y tratamientos depende de forma directa del desarrollo científico alcanzadoa nivel internacional. El prometedor futuro de la investigación sanitaria debe tener en cuenta los principios establecidos en el referido Código de Núremberg y en el Convenio de Oviedo sobre Derechos Humanos y Biomedicina de 1997, a saber, la prioridad del ser humano y de la protección de sus derechos fundamentales sobre los intereses del avance de la ciencia.

Hace dos décadas, la principal amenaza que se cernía sobre el ser humano en relación a la investigación científica procedía de la experimentación con fármacos o procedimientos invasivos. De hecho, los instrumentos legales y éticos diseñados para controlar la investigación y someterla a límites aceptables desde el punto de vista de los derechos humanos, se referían a este tipo de prácticas experimentales que consistían en la intervención física sobre el cuerpo humano. Dos décadas más tarde, la investigación biomédica se impone como especialidad que opera con un componente importante de gestión de datos obtenidos de diversas fuentes. Las potentes herramientas informáticas con las que se procesan las informaciones permiten combinar millones de datos con resultados sorpredentes para los estudios poblacionales y estadísticos. Hoy es prácticamente inexistente la investigación que no se sirve del tratamiento de datos, ya sea de forma sustancial, como elemento esencial, o secundaria, a través del contraste de resultados. La investigación que hace uso de datos sensibles, como los relativos a la salud, incluidos los genéticos o biométricos, debe ser encuadrada en los principios éticos y jurídicos que han emergido en estas dos pasadas décadas. A diferencia de lo que sucedía cuando se redactó el Código de Núremberg o el Convenio de Oviedo, este uso masivo de datos supone hoy una amenaza añadida para el derecho fundamental del ser humano a su autodeterminación informativa y a su intimidad. El riesgo de discriminación en base a la elaboración de perfiles derivados de la captación indiscreta de los datos obtenidos de Internet y de otras fuentes accesibles a los investigadores debe prevenirse, así como se hace necesario un mejor conocimiento por parte de las personas físicas de cuáles son los procedimientos de tratamiento de datos, con el objeto de disponer de una mayor capacidad de control de la protección de datos personales[1].

[1] Jiménez Asensio, Rafael, *Introducción al nuevo marco normativo de la protección de datos personales en el sector público,* Ed. IVAP, Oñati, España, 2019, p. 36.

En este sentido, el ordenamiento español posee una serie de instrumentos jurídicos que han contribuido a enmarcar la investigación con datos sanitarios garantizando un alto estándar de protección de los derechos fundamentales[2]. La Ley 14/2007, de Investigación Biomédica, marcó un hito en el catálogo legislativo que le había precedido, estableciendo pautas concretas para operar con datos provenientes de muestras biológicas. Con todo, la regulación aplicable a la investigación en materia biomédica y de salud en España carecía de un marco general aplicable a la toda aquella investigación científica que operara sobre datos. Las leyes que habían incidido en la materia establecieron pautas sectoriales para el uso de datos provenientes de la historia clínica, de la investigación con embriones o fetos vivos o muertos, con tejidos humanos y gametos, sobre ensayos clínicos con medicamentos o en terapia celular, investigaciones clínicas con productos sanitarios, estudios observacionales sobre medicamentos, etc.; pero, faltaba un marco general regulador de los estudios que se sirven solo o fundamentalmente de datos, cualquiera que sea su procedencia.

En esta coyuntura se promulgó el Reglamento General de Protección de Datos (UE) 2016/679[3], en adelante RGPD, el cual introduce importantes novedades en relación a la investigación sanitaria que se sirve da datos personales. A partir de dicho hito normativo, tras más de un año de tramitación parlamentaria, el BOE del 6 de diciembre publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), cuya entrada en vigor se produjo el día 7 de diciembre. Esta regulación deroga la anterior LOPD de 13 de diciembre de 1999 (LO 15/1999), y el más reciente Real Decreto Ley 5/2018, de 27 de julio, que tenía una vocación puramente transitoria. Mediante tales derogaciones expresas se daba así cumplimiento a la necesaria adaptación normativa del Derecho interno a las previsiones del RGPD.

En el presente trabajo analizaremos las previsiones normativas del binomio Reglamento-Ley Orgánica que se refieren al uso masivo de datos sanitarios en investigación de salud. Para ello, repararemos en primer lugar en la singularidad del nuevo marco legal impuesto por el Reglamento y la Ley Orgánica española que lo complementa. Veremos en qué consisten las

---

[2] CEAB, *Controles éticos en la actividad biomédica. Análisis de situación y recomendaciones*, Instituto Roche, Madrid, España, 2009.

[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).

principales novedades que aporta el Reglamento, cuya primacía sobre el nivel normativo estatal constituye una realidad indiscutida, en materia de protección de datos en general, y sobre la investigación con datos masivos en particular. A continuación, analizaremos en detalle la interpretación y el desarrollo que ha llevado a cabo la LOPDGDD a partir de la remisión legislativa operada por el propio Reglamento en materia de investigación a partir de datos de salud. Y finalmente, incluiremos un anexo en el que se relacionan de forma esquemática los principales pasos que constituyen la nueva ruta de control de las investigaciones con datos en el ámbito sanitario tras la promulgación de los meritados textos normativos.

1. El marco normativo compuesto por el RGPD y la nueva LOPDGDD

El RGPD tiene la particularidad de que sus disposiciones constituyen derecho directamente aplicable. En este sentido se ha dicho que,

> "[…] el RGPD con carácter general tiene primacía aplicativa y entra, asimismo, en una serie de detalles en la regulación sus tantiva tanto de principios, derechos como instrumentos o institucio nes que la propia LOPDGDD solo puede reenviar a lo establecido en aquél. Se podrá comprobar, así como el reenvío, en efecto, es una técnica normativa muy usada por la LOPDGDD, cuando no la propia anomia normativa, al no regular una materia que trata en su práctica totalidad el RGPD. Ambas son técnicas que ponen de relieve la posición vicarial o subordinada de la regulación orgánica frente al Reglamento de la Unión Europea. Pero que complican sobremanera la labor del operador o técnico"[4].

El nuevo Reglamento pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la citada Directiva, cuya trasposición se tradujo "en un mosaico normativo de perfiles irregulares en el conjunto de la Unión Europea"[5], lo que condujo a que existieran diferencias apreciables en la protección de los derechos de los ciudadanos en función del país de origen. No obstante, el Reglamento renuncia armonizar directamente determinados ámbitos, como es el caso de la investigación sanitaria, permitiendo que sus normas sean especificadas o interpretadas por los Estados miembro. Se ha dicho que el Reglamento sienta unas bases

[4] Jiménez Asensio, Rafael, *Introducción al nuevo marco normativo de la protección de datos personales en el sector público, op. cit.,* p. 37.

[5] Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

más sólidas que la Directiva anterior para dar respuesta a las necesidades y a los riesgos aparejados al tratamiento de los datos con fines de investigación biomédica[6]. Sin llegar a desarrollar un régimen jurídico específico para la utilización de datos de salud con fines de investigación científica, el RGPD reenvía a la normativa de los propios Estados, aunque también contempla futuros desarrollos normativos propios "sobre la base del Derecho de la Unión".

No cabe duda de que esta delegación frustra en gran medida las expectativas de armonización directa que abrigaban los grupos e instituciones investigadoras, necesitadas de unas normas homogéneas de funcionamiento en una materia tan internacionacionalizada como es la investigación en salud[7]. Con todo, es innegable que el nuevo enfoque es más adecuado y constituye un buen punto de partida. El Reglamento establece principios adecuados para que se desarrolle dicha colaboración internacional sin merma de los derechos de los pacientes y de los titulares de los datos sanitarios. Dichos principios deberán ser interpretados por los Estados miembro de la Unión, los cuales están llamados a tener en cuenta la dimensión internacional de la investigación biomédica y la necesidad de establecer marcos jurídicos adecuados para garantizar el desarrollo y la profundización de dicha colaboración. Este nuevo marco está empezando a dibujarse a través de los desarrollos normativos que ya se han implementado en países miembro como Reino Unido[8], Alemania[9] o la propia España, con la promulgación de la nueva LOPDGDD, cuyas normas deberían ser referentes para el resto de los Estados miembro a la hora de aprobar su propia normativa.

El Reglamento indica que la adhesión a códigos de conducta o a un mecanismo de certificación de los previstos en el mismo podrá ser utilizada para demostrar el cumplimiento de las obligaciones por parte del Responsable del tratamiento. Es por tanto previsible que tras la aprobación del Reglamento y de las leyes nacionales, se abrirá una tercera fase en materia de investigación

---

6 Chico, V., "The impact of the General Data Protection Regulation on health research", *British Medical Bulletin*, Núm. 1, Vol. 128, 2018, pp. 109-118.

7 Reichel, Jane, "Oversight of EU medical data transfers – an administrative law perspective on cross-border biomedical research administration", *Health Technol.* 7, 2017, pp. 389-400.

8 Data Protection Act 2018. Disponible en: https://services.parliament.uk/bills/2017-19/dataprotection.html

9 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097). Disponible en: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117044.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117044.pdf%27%5D__1555085841351

biomédica a través de las recomendaciones emitidas por el nuevo Comité Europeo de Protección de Datos y, eventualmente, gracias a los Códigos tipo que el sector estará en condiciones de aprobar en el medio plazo[10].

2. Principales novedades introducidas en el RGPD

El aspecto más novedoso del Reglamento consiste en incidir sobre la obligación de prevención por parte de las organizaciones que tratan datos[11]. Con el nuevo régimen de tratamiento de los datos se pretende transitar de una cultura de gestión y control administrativo previo a una autogestión Responsable de los riesgos, con rendición posterior de cuentas. Es significativa al respecto la redacción del Considerando 89, según el cual:

> "La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el Responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial".

El artículo 30 del Reglamento elimina por tanto la obligación que obrara en la Directiva anterior de notificar la creación de ficheros de datos a la autoridad de control. En su lugar, la nueva normativa incita a un mayor compromiso de las organizaciones, tanto públicas como privadas, con la prevención[12]. Es lo que se conoce como responsabilidad proactiva. La idea

---

[10] Aced Félez, Emilio, "Protección de Datos y Transformación Digital en Sanidad", *Revista de la sociedad española de informática y salud*, Vol. 118, 2016.

[11] Masse, Estelle, *General Data Protection Regulation – what tidings do ye bring?,* 21 December 2015. Disponible en: https://www.accessnow.org/general-data-protection-regulation-what-tidings-do-ye-bring/.
Jiménez Asensio, Rafael, *Introducción al nuevo marco normativo de la protección de datos personales en el sector público,* Ed. IVAP, Oñati, España, 2019.

[12] González, P., "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata*, Núm. 24, 2017, pp. 115-129.

de la responsabilidad proactiva (*accountability*), de origen anglosajón, se condensa en el Considerando 78 del Reglamento según el cual:

> "A fin de poder demostrar la conformidad con el presente Reglamento, el Responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto".

Los Responsables de los datos deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece (artículo 24). Se entiende que en la era de Internet, actuar sólo cuando se ha producido una infracción es insuficiente, dado que el daño causado a los interesados puede ser muy difícil de compensar o reparar. En este sentido, se prevén importantes novedades como la introducción temprana en las organizaciones de políticas de privacidad de los datos, la evaluación previa del impacto de los tratamientos planeados, medidas de seguridad, mantenimiento de un registro de tratamientos en el caso de organizaciones de más de 250 trabajadores, nombramiento de un Delegado de protección de datos, elaboración de códigos de conducta y esquemas de certificación, consulta previa a las autoridades de control, notificación de los incidentes y de las brechas de seguridad, etc. Esta cultura de la protección desde el diseño se hace extensiva a los productores y proveedores con los que se trabaja, ya sean empresas o administraciones, las cuales deberán poder asegurar que están dotadas de políticas y herramientas de protección de datos (Considerando 78).

No obstante, a la hora de acomodarse al nuevo paradigma, debe tenerse en cuenta que la cultura de la *accountability*, es nueva y desconocida para el derecho continental, el cual se basa, como es sabido, en un sistema de acreditación mediante la autorización administrativa previa. La adopción del sistema anglosajón del que proviene el nuevo paradigma de responsabilidad adoptado por el Reglamento presupone que los países europeos están preparados para omitir el control previo. Sin embargo, con este proceder se está obviando el problema de que en los sistemas continentales no se dispone de los mismos recursos para la pesquisa y la investigación de los hechos *a posteriori* que en el sistema administrativo y judicial anglosajón[13].

[13] Alhadeff, J. / Van Alsenoy, B. / Dumortier, J., "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions", *Managing Privacy through Accountability*, Guagnin, D. / Hempel, L. / Ilten, C. / Kroener, I. / Neyland, D. / Postigo, H. (Eds), Palgrave Macmillan, Londres, Reino Unido, 2012.

2.1. Enfoque basado en la protección de riesgos

El Reglamento señala que a fin de poder demostrar la conformidad con el estándar de protección exigible, el Responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan los principios de protección de datos "desde el diseño". El artículo 25 define la *protección desde el diseño y por defecto* como la obligación del Responsable del tratamiento de aplicar, tanto en el momento de determinar los medios para el tratamiento, como durante el mismo, las medidas técnicas u organizativas adecuadas, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratramiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas (artículo 25.1 RGPD).

En concreto, la responsabilidad proactiva exige (Considerando 78) que la empresa u organización adopte medidas de seguridad en relación con la seudonimización; el cifrado, dirigido a impedir el acceso a los mismos a las personas no autorizadas; la confidencialidad, la integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a datos personales de forma rápida en caso de incidente físico o técnico; y el proceso de verificación, evaluación y valoración periódica de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En cuanto a la obligación de la "protección de datos por defecto", señala el apartado segundo del artículo 25 que:

> "El Responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".

Para cumplir con el principio de minimización referido, habrá que definir qué datos se van a utilizar, dónde se van a almacenar, quién va a coordinar el procesamiento y para qué se van a utilizar. Preguntas básicas para las que debe estar preparada cualquier organización que quiera implementar tratamientos de datos a gran escala.

2.2. Evaluación de impacto

Es preciso tener en cuenta, como se ha dicho, que la mayor novedad que presenta el Reglamento es la evolución de un modelo basado en el control del

cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el Responsable o por el Encargado de la gestión del riesgo que pueda generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan.

El RGPD consagra, por tanto, un modelo de cumplimiento basado en la gestión enfocada al riesgo. La *Evaluación de Impacto en la Protección de Datos Personales* (EIPD) se erige así en clave de bóveda para poder justificar y evaluar las decisiones; de ser una herramienta procedimental interna, la EIPD pasa a ser elemento sustancial en la configuración del estándar de cumplimiento de la protección[14]. El Reglamento prevé que antes del tratamiento, el Responsable debe llevar a cabo una EIPD con el fin de valorar la particular gravedad y probabilidad de riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento así como los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el Reglamento (artículo 35). Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que proyectan tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional, y que podrían afectar a un gran número de interesados. La evaluación de impacto debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas basadas en la elaboración de perfiles a partir de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, como datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas (Considerando 91 y artículo 35.3 RGPD).

Se prevé que la autoridad de control establezca y publique una lista de los tipos de operaciones concretas que requieran evaluación de impacto (artículo 35.4 RGPD). Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en

[14] La Evaluación del Impacto se contemplaba ya en el artículo 27 de la Directiva (EU) 2016/680 en la que se establecía que dicha evaluación del impacto del tratamiento sobre la privacidad es exigible cuando "el tratamiento puede resultar en un alto riesgo para la libertad de las personas físicas". La Agencia Española de Protección de Datos publicó en 2017 una Guía para la Evaluación de Impacto en la Protección de Datos Personales que sirve de referencia en materia de requisitos técnicos y procedimentales que debe reunir una EIPD. AEPD, Guía para la Evaluación de Impacto en la Protección de Datos Personales. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf.

cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

En el futuro se podrán proporcionar directrices que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité Europeo de Protección de Datos o indicaciones proporcionadas por un Delegado de protección de datos. El Comité también puede emitir orientaciones sobre operaciones de tratamiento que no supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

Además de esta cautela, el artículo 36 del Reglamento prevé que el Responsable deberá consultar a la autoridad de control competente antes de iniciar las actividades de tratamiento en el caso de que la EIPD muestre que el tratamiento entraña un alto riesgo para los derechos y libertades de las personas físicas que no puede mitigarse por medios razonables en términos de tecnología disponible y coste de la aplicación de la misma. En estos casos, la autoridad de control estatal o autonómica competente deberá asesorar por escrito al Responsable o al Encargado en un tiempo de ocho semanas desde la realización de la consulta, y podrá utilizar sus poderes de investigación o correctivos contemplados en la normativa. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada al Responsable, cuyas piezas principales se detallan en el propio Reglamento (artículo 36.3).

Finalmente, recuérdese que el artículo 36 requiere que los Responsables del tratamiento consulten a la autoridad de control incluso si no se da dicho alto riesgo, puesto que el Estado miembro puede requerir al Responsable que consulte y en su caso obtenga una autorización previa de la autoridad de control independiente cuando se trate de tratamientos relacionados con datos sensibles como es el caso de la sanidad (artículo 36.5).

2.3. Quiebras de seguridad y notificación

Las medidas previstas en los artículos 33 y 34 del Reglamento constituyen una de las novedades más relevantes en materia de seguridad. En estos artículos se regula el deber que atañe a todos los Responsables de comunicar la violación de seguridad que se produzca en los sistemas cuando los ataques o los accidentes conlleven la destrucción, pérdida, alteración, acceso o

comunicación no autorizada de los datos. A fin de minimizar dichos riesgos, la empresa u organización debe contar con medios ágiles de detección y notificación de las violaciones; y se le exige, además, implementar un plan de contingencia que permita reducir el impacto de los daños de forma rápida.

Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reidentificación de datos, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona en cuestión. Por consiguiente, tan pronto como el Responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el Responsable debe, sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida (Considerando 85).

La notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el Reglamento (Considerando 87).

El Responsable del tratamiento debe comunicar también al interesado la violación de la seguridad de los datos personales en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, con el fin depermitirle tomar las precauciones necesarias. La comunicación al interesado debe incluir una descripción dela naturaleza de la violación de la seguridad de los datos personales y contener también las recomendaciones para que la persona física afectada pueda mitigar los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabría justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones continuas o similares de la seguridad de los datos personales (Considerando 86).

3. Tratamiento de datos con tecnologías Bigdata

El RGPD no define qué debe entenderse por Bigdata, aunque en su Considerando 91 hace referencia a:

> "…las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional, y que podrían afectar a un gran número de interesados y entrañen probablemente alto riesgo, por ejemplo, debido a su sensibilidad".

Esta aproximación plantea dos cuestiones que resulta necesario aclarar con el fin de definir qué se entiende por *Bigdata* en el ámbito sanitario. Uno de los problemas consiste en determinar el propio alcance de la expresión "tratamiento masivo de datos" o "tratamiento de datos a gran escala"; además, también resulta necesario clarificar qué tipos de datos pueden entenderse comprendidos en este ámbito. En concreto, se duda si los datos anonimizados de salud deben ser objeto de protección cuando forman parte de un proyecto *Bigdata.*

3.1. Tratamiento masivo de datos o tratamiento de datos a gran escala

El referido Considerando 91 del RGPD al que ya hemos hecho referencia menciona como elementos integrantes del concepto de tratamiento de datos "a gran escala":

- el número de titulares de datos concernidos, tanto en términos absolutos como en términos de proporción en relación a una población determinada,

- el volumen de datos o/y el rango de los items procesados,

- la duración, o la permanencia del tratamiento en el tiempo,

- la extensión geográfica de la actividad de procesamiento,

Por otra parte, el mismo Considerando 91 establece específicamente que "el tratamiento de datos personales no debe considerarse a gran escala si el procesamiento lo realiza, respecto de datos personales de un paciente o clientes, un solo médico u otro profesional de la salud o abogado."

Como se ha visto, el Reglamento ofrece ejemplos de tratamientos de datos en masa en los dos extremos de la escala (desde el procesamiento de datos por parte de un solo profesional de la salud en relación a los datos de sus pacientes, al tratamiento de datos de todo un país o continente). Entre ambos extremos, existe, como es obvio, una amplia zona gris.

En relación con el procesamiento de datos de salud "a gran escala", el Grupo de Trabajo del artículo 29 considera tratamiento a gran escala "el procesamiento habitual de datos de los pacientes en un hospital" [15]. También incluye en este tipo de tecnologías Bigdata el tratamiento de datos recabados por proveedores de servicios de telefonía e internet (contenidos, tráfico, geolocalización, etc.).

3.2. Datos anonimizados y seudonimizados

En relación al tratamiento masivo de datos, el Grupo de Trabajo del artículo 29, en adelante GT29, entendió en su *Declaración relativa al tratamiento de datos a gran escala*, adoptada con anterioridad a la adopción del nuevo Reglamentoque estos tratamientos requieren una atención particular, incluso cuando los datos hayan sido previamente anonimizados,

> "…la conservación y el análisis de grandes cantidades de datos personales anonimizados en entornos Bigdata requiere particular atención y cuidado. Estos tratamientos pueden dar como resultado la identificación de perfiles individuales específicos, sobre todo cuando se combinan con una potencia de procesamiento creciente y nuevas técnicas de minería de datos" [16].

Para determinar si una persona es identificable, añade el mismo GT29, "deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el Responsable del tratamiento o cualquier otro individuo para identificar directa o indirectamente a dicha persona", haciendo con ello referencia tanto a la tecnología disponible en el momento del tratamiento

---

[15] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Data Protection Officers ('DPOs')*, Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017. Disponible en: file:///C:/Users/portatil/Downloads/wp243_rev01_enpdf.pdf. p. 21.

[16] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Statement of the WP29 on the impact of the development of Bigdata on the protection of individuals with regard to the processing of their personal data in the EU* WP 221, 14/EN, Adopted on 16 September 2014. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

como a los avances tecnológicos, junto a todos los factores objetivos, como los costes y el tiempo necesario para la identificación[17].

A todas luces, el Reglamento se ha rendido a la evidencia de que ante el progresivo aumento de la capacidad de procesamiento y de cruce de datos anonimizados es imposible en la actualidad, y menos en el futuro, seguir manteniendo la idea de que se pueden anonimizar los datos de forma irreversible, dado que, al final, cualquier dato suficientemente enriquecido y combinado con otros, es susceptible de ser reidentificado. Por este motivo, a diferencia de lo que ocurría en la Directiva anterior, el nuevo Reglamento renuncia a incluir en el listado de definiciones el término "anonimización"[18]. El Reglamento introduce en su lugar el término "seudonimización" en el listado de definiciones. Su artículo 4 recoge la definición del mismo en los siguientes términos:

> "El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Podría decirse, por tanto, que el estándar europeo de protección de datos resulta de una definición contextual del término "identificación" en relación al estado de la técnica. Esto supone que aunque los datos estén doblemente codificados por un tercero de confianza (*key-coding*) y los investigadores no puedan re-identificar los datos por sí mismos (la norma exige que los ficheros que contienen los códigos de identificación no estén bajo la custodia de la misma organización que detenta los ficheros anonimizados), con todo, estos datos seguirán considerándose "identificables" y, por tanto, seguirán estando

---

[17] Esta definición procede de la Opinión emitida por el Grupo de Trabajo del Artículo 29 en su Informe 05/2014. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, Adopted on 10 April 2014. https://www.pdpjournals.com/docs/88197.pdf. Véase así mismo sobre el concepto de dato anónimo, el Informe Jurídico en relación a la dirección IP de la AGENCIA ESPAÑOLA DE PROTECCIÓN DATOS. AEPD, *Carácter de dato personal de la dirección IP.* Informe 327/2003. Disponible en: https://www.aepd.es/informes/historicos/2003-0327.pdf

[18] No obstante, el Considerando 26 sigue declarando, como hacía la Directiva derogada, que los principios de protección de datos no deben aplicarse a la información anónima. Es más, por esta vía se quiere "liberar" datos permitiendo su libre circulación y comercialización como base de la economía digital que contribuye fuertemente al PIB europeo. Véase a título de ejemplo la reciente propuesta de regulación en materia de libre circulación de datos anonimizados, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the free flow of non-personal data in the European Union COM/2017/0495 final - 2017/0228 (COD).

dentro del ámbito de aplicación del Reglamento siempre que puedan ser re-identificados con un "esfuerzo razonable" (Considerando 26).

El término "seudonimización" no se contemplaba en la redacción inicial del borrador que realizó la Comisión. Una vez adoptado el término, su definición fue muy fluctuante a lo largo de la tramitación del Reglamento. El concepto finalmente acordado fue en realidad fruto de un acerado debate en el Trilogue entre las tres instituciones implicadas, Comisión, Consejo y Parlamento[19]. Algunas inconsistencias en la regulación, que analizaremos más adelante, dan fe de las numerosas enmiendas y contra-enmiendas que hubo que tramitar y de los equilibrios a los que se llegó tras la azarosa tramitación[20]. La propuesta alemana, que fue finalmente adoptada, consistía en recuperar la idea del enfoque proporcional al riesgo (*risk proportionate approach*), con la intención declarada de incentivar la mejora y sofisticación de las técnicas de seudonimización que permitan ofrecer mayores garantías a los interesados permitiendo al mismo tiempo el uso de datos seudonimizados para la investigación[21].

Algunos comentaristas han señalado que la sustitución operada por el Reglamento entre anonimización y seudonimización no es anodina[22]. Con la nueva normativa, no es necesario anonimizar los datos; bastaría con que hayan sido seudonimizados para poder emplearlos con finalidades de interés

---

[19] El debate de las Trilogue no se hace público, si bien la Comisión pública una nota de prensa en la que se recoge un resumen de las cuestiones tratadas. *Agreement on Commission's EU data protection reform will boost Digital Single Market*, Brussels, 15 December 2015, European Commission.

[20] *Impact of the draft European Data Protection Regulation and proposed amendments from the rapporteur of the LIBE committee on scientific research*, 2013.

[21] [Proposal GER] Art. 83. "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a controller to which the data are disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. In assessing the interests it should be taken into account that the controller or personnel of the controller has taken effective measures of seudonymisation of personal data in order to minimize the risk of the data subject. In such cases there is a refutable presumption that the subject's interests and fundamental rights and freedoms do not override the controller's interests. This subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks." Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM/2012/011 final - 2012/0011 (COD).

[22] Moerel, Lokke / Prins, Corien, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (May 25, 2016). Disponible en: https://ssrn.com/abstract=2784123 or http://dx.doi.org/10.2139/ssrn.2784123

público, de investigación científica e histórica, o estadísticos, sin necesidad de recabar de nuevo el consentimiento del interesado. El texto finalmente adoptado refleja el nuevo equilibrio alcanzado entre las instituciones europeas para permitir la libre circulación de los datos, especialmente en materia de investigación, cifrando, como veremos más adelante, el nivel de seguridad exigido en un grado de disociación acorde con el estado de la técnica en cada momento.

3.3. Adopción de medidas técnicas y organizativas

Con carácter general, según prevé el artículo 24.1 del RGPD, el Responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa aplicable, y lo hará teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, debiendo considerar de forma especial los principios de privacidad por diseño y por defecto en este ámbito.

La política deprotección de datos, el protocolo de actuación y las medidas tecnológicas adoptadas respecto de los procedimientos de anonimización o seudonimización habrán de reforzarse con las garantías jurídicas necesarias para preservar los derechos de los interesados. Dichas garantías jurídicas pueden consistir, por ejemplo, en acuerdos de confidencialidad y cláusulas contractuales que garanticen la privacidad de la información –incluso cuando haya brechas de seguridad que provoquen la reidentificación de los datos–; en compromisos de mantenimiento de la anonimización de la información suscritos con los posibles destinatarios de la misma así como en la promesa de no realizar ninguna acción para re-identificarla; o auditorías de uso de la información anonimizada.Estas garantías serán tenidas en cuenta como parte de las salvaguardas adoptadas para la minimización de los daños ante una eventual reidentificación de los interesados.

En último lugar, la AEPD recomienda la realización de un proyecto piloto con una pequeña muestra de datos de prueba (no reales) del que puedan extraerse, de forma objetiva, conclusiones con respecto a la vialidad de las técnicas de anonimización propuestas y del procedimiento de anonimización o seudonimización[23].

[23] Agencia Española de Protección de Datos, *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD*, 2016. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf.

Además de planificar y adoptar las referidas medidas, el Responsable debe informar de forma específica a la autoridad de control sobre las concretas medidas y garantías que estime adoptar en proyectos Bigdata, debiendo la autoridad de control informar y asesorar al Responsable en caso de que considere que éste no ha identificado o mitigado suficientemente el riesgo con las medidas que haya proyectado. Todo ello en coherencia con lo previsto en el artículo 57.1 del RGPD.

Recuérdese que la nueva Ley Orgánica de Protección de Datos en su número 73.d considera infracción grave la falta de adopción de las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25.2 del Reglamento (UE) 2016/679[24].

3.4. Funciones encomendadas a las instancias encargadas de supervisar los proyectos de tratamientos Bigdata

A partir del nuevo paradigma instaurado por el Reglamento General de Protección de Datos, basado, como se ha dicho repetidamente, en la responsabilidad activa y la prevención de los riesgos ligados al tratamiento de los datos en entornos Bigdata, se plantea a continuación la función asignada en este nuevo modelo a las autoridades de control y a la nueva figura del Delegado de Protección de Datos[25]. Como se verá, ambas instancias ven acrecentadas su labor de consulta y asesoramiento previo en detrimento de las funciones de control administrativo asignadas en la regulación anterior. Al mismo tiempo, y en consonancia con el principio de responsabilidad activa de los Responsables del tratamiento, las Agencias refuerzan su competencia sancionatoria, cuyas cuantías aumentan ostensiblemente en relación a la tabla anterior.

---

[24] Hasta la promulgación de la nueva LOPDGDD, e incluso después, el vacio normativo y las dudas interpretativas han sido colmadas en gran parte gracias a la encomiable labor realizada por las Agencias de Protección de Datos. Cabe mencionar por parte de la AEPD la Guía para la gestión y notificación de brechas de seguridad, Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos a RGPD, Código de Buenas Prácticas en Protección de Datos para proyectos Big Data, Orientaciones y garantías en los procedimientos de anonimización de datos personales, entre otros. Por parte de la Agencia Vasca de Protección de Datos, Guía del Reglamento General de Protección de Datos para responsables de tratamiento, etc.

[25] Mostert, Menno / Bredenoord, Annelien L. / Van Der Slootb, Bart / Van Deldena, Johannes J.M. "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", *European Journal of Health Law*, Vol. 25, 2018, pp. 43-55.

3.4.1. Delegado de Protección de Datos

El Reglamento crea la figura del Delegado de Protección de Datos (*Data protection officer* DPO, en sus siglas en inglés) en sus artículos 37 a 39.

El RGPD señala de forma genérica los casos en los que resulta obligatoria la designación de un Delegado de Protección de Datos, indicando entre los mismos a aquellos en los que "las actividades principales del Responsable o del Encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9…" (Artículo 37). La LOPDGDD, por su parte, explicita estos supuestos de obligatoriedad, entre los cuales menciona expresamente a los centros sanitarios, en tanto estén obligados al mantenimiento de historias clínicas, exceptuando "a los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual".

Según la citada normativa, la organización podrá designar un DPO interno o externo, atendiendo a sus cualidades profesionales con el fin de asesorar a la empresa u organización en lo relativo a la normativa de protección de datos. Esta figura debe actuar como punto de contacto para los interesados y las autoridades de control, por lo que deberá contar con los recursos necesarios y autonomía en su gestión. Así lo recoge también la nueva ley orgánica de protección de datos, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrados en la organización del Responsable o Encargado, y ser tanto una persona física como una persona jurídica

Con el fin de garantizar su independencia, el Responsable o el Encargado deberán dotar al Delegado de medios materiales y personales suficientes y no podrán removerle, salvo en los supuestos de dolo o negligencia grave. En concreto, el Reglamento prevé que el Responsable debe velar por la independencia del Delegado, ocupándose de que este no reciba ninguna instrucción externa en lo que respecta al cumplimiento de sus funciones. En particular, no podrá ser destituido ni sancionado por el Responsable en el desempeño de sus funciones, y rendirá cuenta directamente al mismo nivel jerárquico que el propio Responsable o Encargado del tratamiento (artículo 38.3). La Ley española añade que "el Delegado de protección de datos no podrá ser removido ni sancionado por el Responsable o el Encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio" (LOPDGDD, artículo 36.2)

El Reglamento prevé que el Delegado se ocupará como mínimo las siguientes cuestiones:

- informar y asesorar al Responsable de las obligaciones derivadas de la normativa aplicable;

- supervisar el cumplimiento de dicha normativa y de las políticas de protección de datos de la organización, incluida la sensibilización y formación del personal;

- cooperar con la autoridad de control, actuando como interlocutor del Responsable o Encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos (LOPDGDD, artículo 36.1);

- ofrecer el asesoramiento solicitado en la evaluación de impacto y supervisar su aplicación.

En relación a este último supuesto, el Reglamento preve expresamente la implicación temprana del Delegado y especifica que el Responsable debe recabar el consejo del Delegado al realizar las evaluaciones de impacto[26]. El GT29 recomienda en su Guía de abril de 2017, sobre el Delegado de Protección de Datos, que el Responsable consulte con el DPD en los aspectos fundamentales del tratamiento previsto[27]. Si el Responsable discrepa en relación a la opinión del Delegado, dicha discrepancia debería hacerse constar por escrito en el mismo documento que recoge la EIPD, especificando que la opinión del Delegado no ha sido tenida en cuenta.

Además, se ha indicado que el DPD debe "cooperar con la autoridad de control" y "actuar como punto de contacto con aquella en los asuntos relativos al procesamiento, incluida la consulta previa a la que se refiere el artículo 36" (artículo 39. 1. d). De esta manera, el DPD actúa como facilitador de las tareas de control mencionadas en el artículo 57, como el acceso a la información, auditoría, autorización y asesoramiento practicadas por la Autoridad de Control.

---

[26] El artículo 35 (2) establece que la el Delegado deberá ser informado y consultado desde el principio para facilitar el cumplimiento del Reglamento, promoviendo una política de privacidad desde el diseño y, por lo tanto, esta implicación debe ser el procedimiento estándar de gobernanza de la organización.

[27] Article 29 Data Protection Working Party *Guidelines on Data Protection Officers ('DPOs')* 243 /2016.

El Delegado está sometido al secreto profesional y a la confidencialidad en el desempeño de sus funciones, siguiendo las reglas del derecho del Estado miembro (artículo 38). Sin embargo, la obligación de secreto y confidencialidad no debe impedir que el Delegado ejerza su función de punto de contacto y consulta previa a la autoridad de control siempre que lo estime oportuno (artículo 39.1). Además de la relación con la Agencia, el Delegado debe actuar como intermediario con los agentes relevantes del entorno como los propios usuarios, los proveedores, las unidades de negocio de las organizaciones, etc. Es de destacar que el Delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el Responsable o Encargado del tratamiento.

Se ha mencionado también que el Delegado es el Encargado de fomentar la cultura del respeto a la protección de datos dentro de la organización, organizando las actividades de sensibilización y formación que estime oportunas.

Es preciso subrayar que los Delegados no son Responsables en caso de violación del Reglamento. La norma establece claramente, como se ha dicho, que el Responsable o el Encargado, en su caso, serán los que respondan de las infracciones, y será a ellos quienes se dirijan las autoridades competentes a la hora de solicitar las pruebas que demuestren su cumplimiento.

La designación del Delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La ley orgánica prevé que la Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los Delegados de protección de datos, accesible por cualquier persona.

3.4.2. Autoridades de control

Las autoridades nacionales de control juegan un papel primordial en la protección y la garantía del derecho fundamental a la protección de datos de carácter personal, debiendo éstas velar por el mismo, tal y como reconoce el propio TJUE[28], en aplicación de las facultades que aquéllas ostentan en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y del nuevo

[28] Entre otros pronunciamientos jurisprudenciales acerca de la importancia de las funciones y misión actual de las autoridades de control destaca, en particular, la Sentencia TJUE en el asunto C-362/14 Maximillian Schrems/Data Protection Commissioner. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf.

paquete regulatorio europeo en este ámbito, en particular, contenidas en el RGPD en sus artículos 51 y siguientes.

En este sentido, el Reglamento reconoce de forma expresa que el establecimiento en los Estados Miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de sus datos de carácter personal. El artículo 54 del RGPD prevé que cada Estado miembro establecerá por ley las normas y procedimientos para la designación de los miembros de dichas autoridades. Las funciones vienen detalladas en el propio Reglamento, artículo 57, y van desde "controlar la aplicación del Reglamento e investigar su cumplimiento" hasta la "elaboración de códigos de conducta y cláusulas contractuales tipo", pasando por la "imposición de sanciones como consencuencia de la infracción de las previsiones del presente Reglamento".

Atendiendo a dicho mandato y conservando al mismo tiempo el esquema que se venía recogiendo en sus antecedentes normativos, la Ley Orgánica regula el régimen de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, así como la cooperación entre las autoridades de control (Título VI). En concreto, la LOPDGDD prevé que las funciones contempladas en los artículos 57 y 58 del Reglamento se ejercerán en función del reparto competencial contemplado en los respectivos Estatutos de Autonomía, con respecto de los cuales la Agencia Española de Protección de Datos se coloca en una posición de subsidiariedad.

El Reglamento establece que deberá consultarse a la autoridad de control competente antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el Responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación (artículo 36).

Los Estados miembros podrán establecer la obligación dirigida a los Responsables del tratamiento de consultar a la autoridad de control y a recabar en todo caso su autorización previa cuando se trate de proyectos de tratamiento de datos relacionados con la protección social y la salud pública (artículo 36. 5). No es el caso de la investigación biomédica que ni

en el Reglamento ni en la LOPDGDD se contempla como actividad sujeta a autorización previa.

No obstante, recuérdese que dicha EIPD así como la consulta previa –obsérvese que no se trata de una exigencia de autorización sino de mera consulta– a la Autoridad de control se contemplan en el caso de que "se produzca un tratamiento masivo de datos que implique a un gran número de afectados o conlleve la recogida de un gran número de datos personales" (artículo 28. 2. f de la Ley Orgánica 3/2018).

La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas (artículo 36).

Por otra parte, la LOPDGDD prevé en su artículo 42 que estarán sometidas a autorización previa de las autoridades de protección de datos competentes las transferencias internacionales de datos que no cuenten con una decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en la Ley Orgánica (supuestos de adopción de cláusulas tipo por la Agencia Española de Protección de Datos). Y, en cualquier caso, los Responsables del tratamiento deberán informar con carácter previo a la AEPD o a las autoridades autonómicas competentes de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos (artículo 49.1 RGPD).

En conclusión, puede afirmarse que los proyectos internacionales de investigación en salud que impliquen un tratamiento de datos a gran escala estarán siempre sometidos a la autorización previa de la Agencia competente.

3.4.3. Registro de actividades de tratamiento y de cesión

En cumplimiento del artículo 30 del RGPD, resulta obligatorio que el Responsable, en el caso de desarrollar un proyecto Bigdata, cuente con

un Registro de las actividades de tratamiento asociadas al mismo, el cual, quedará a disposición de la autoridad de control competente.

Este registro será obligatorio para entidades con más de 250 trabajadores, e incluso también para las que empleen a menos personas en el caso de que el tratamiento proyectado pueda entrañar un riesgo para los derechos y libertades de los interesados (y ya se ha visto que los proyectos Bigdata pueden comportar este riesgo debido a la posibilidad de reidentificación de datos anonimizados o seudonimizados), no sea ocasional, e incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, que como sabemos comprende específicamente los datos genéticos y los de salud.

El artículo 31 de la LOPDGDD establece al respecto que "el registro podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado Reglamento".

Además, de acuerdo con el artículo citado, el Responsable o el Encargado estarán obligados a comunicar al DPD cualquier adición, modificación o exclusión en el contenido del registro; y en el caso de que se trate de un organismo público, deberán hacer público un inventario de sus actividades de tratamiento que sea accesible por Internet (artículo 31.2 LOPDGDD).

3.4.4. Notificación por el Responsable o el Encargado del tratamiento de una posible violación de la seguridad de los datos personales

Tal como se ha dicho más arriba, en caso de que se produzca una violación de la seguridad de los datos vinculados a un proyecto Bigdata de conformidad con el artículo 33 del Reglamento, el Resposable deberá comunicar la misma a la autoridad de control que corresponda. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el Reglamento (Considerando 87). El incumplimiento de dicha notificación es considerado por la Ley Orgánica 3/2018 una infracción grave (artículo 73, r).

El Responsable del tratamiento debe comunicar al interesado la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, con el fin de que pueda, por su parte, tomar las precauciones necesarias.

4. Utilización de datos personales con fines de investigación

La regulación del tratamiento de los datos destinados la investigación científica ha sido uno de los caballos de batalla en la elaboración del Reglamento General de Protección de Datos finalmente aprobado. Se debatió, en particular, la investigación en materia de salud y biomédica a la cual el programa marco europeo de investigación (Horizonte 2020) dedica una cantidad muy importante de recursos. El Consejo Europeo y los propios investigadores esgrimieron razones de peso para hacer de la investigación una base legal que autorice el tratamiento de los datos sanitarios. El resultado de esta tensión entre el mantenimiento de un alto estándar en materia de protección de datos, como corresponde al ámbito europeo regido por su Carta de Derechos Fundalmentales, por una parte, y la voluntad de favorecer la investigación y el conocimiento, por otra, tiene su reflejo en un texto normativo fruto de un iter legislativo profusamente enmendado, que da como resultado una regulación compleja, cuyo significado no es siempre fácil de interpretar.

4.1. ¿Qué se entiende por "investigación científica"?

Una primera dificultad a la hora de interpretar la nueva regulación relativa a la investigación sanitaria estriba en el alcance que el Reglamento otorga al propio término de investigación.

El Considerando 159 hace referencia al uso de datos en la investigación científica en general, explicando que:

> "… El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1 del Tratado de Funcionamiento de la Unión Europea de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública...".

Parece por tanto que el Reglamento, tanto de forma directa como a través de la invocación del Tratado de Funcionamiento, aboga por una intelección amplia de la investigación científica[29]. El propio Considerando

[29] El referido artículo 179 (1) del Tratado de Funcionamiento de la Unión Europea establece que: "La Unión tendrá por objetivo fortalecer sus bases científicas y tecnológicas,

159 se refiere tanto a la investigación pública como a la privada, sea aplicada o básica. La referencia al artículo 179 (1) del Tratado podría interpretarse en el sentido de que la norma parece exigir en todo caso, tanto para la investigación pública como para la aplicada en el dominio privado, que se pueda acceder al resultado de la investigación a través de la publicación o de otro medio que garantice "la libre circulación de los conocimientos científicos y tecnológicos".

En este mismo sentido, el Reglamento específica que la investigación y la publicación de los resultados deben respetar "las normas éticas reconocidas en la investigación científica" (Articulo 89 y Considerando 33). Si bien algunos campos, como el de la salud, están encuadrados en las directrices emanadas por organismos internacionales como el Council for International Organizations of Medical Sciences (CIOMS) lo cierto es que las normas éticas de la investigación y de su publicación, en sentido amplio, carecen de un marco normativo armonizado a nivel europeo[30]. El Reglamento, como hemos visto tampoco específica las pautas. La falta de definición propia dará sin duda pie a interpretaciones diversas, sobre cuyos límites es probable que deba pronunciarse el Comité Europeo de Protección de Datos.

4.2. La investigación como base legal específica para el tratamiento de datos personales

Una importante autorización que presenta el Reglamento consiste en dotar a la investigación científica de base legal específica para el tratamiento de datos sin necesidad de otra justificación que la satisfacción del interés legítimo perseguido por el Responsable. En efecto, el artículo 6 (1) (f) del Reglamento establece que el tratamiento de los datos será lícito "cuando el procesamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable o el tercero".

El concepto de "interés legítimo" sobre el que se basaba también la Directiva para autorizar el procesamiento dirigido a la investigación fue objeto

---

mediante la realización de un espacio europeo de investigación en el que los investigadores, los conocimientos científicos y las tecnologías circulen libremente, y favorecer el desarrollo de su competitividad, incluida la de su industria, así como fomentar las acciones de investigación que se consideren necesarias en virtud de los demás capítulos de los Tratados".

[30] Tene, Omar / Polonetsky, Jules, "Beyond IRBs: Ethical Guidelines for Data Research", 72 *Wash. & Lee L. Rev. Online* 458, 2016. Abiduzzaman, M. *et ál.*, "Big data in healthcare –the promises, challenges and opportunities from a research perspective: a case study with a model database", *AMIA. Annual Symposium proceedings. AMIA Symposium.* Vol. 2017, pp. 84-392.

de interpretación por parte del G29, según el cual, "el procesamiento de los datos con fines de investigación, incluida la investigación de mercado, puede constituir una base legal para el tratamiento siempre que el Responsable implemente las garantías oportunas"[31]. En similares términos se pronuncia actualmente el Considerando 47 del Reglamento, que se fija, sobre todo, en el contexto de la recogida de los datos. A título de ejemplo, dice el Considerando citado que "el interés legítimo podría darse cuando existe una relación pertinente y apropiada entre el interesado y el Responsable", y continúa diciendo que "la existencia de un interés legítimo requeriría una evaluación meticulosa" atendiendo también al hecho de que "el interesado pueda prever de forma razonable, en el momento y en el contexto de la recogida de los datos, que pueda producirse un tratamiento con tal fin". En cualquier caso, la apreciación del interés legítimo requiere una ponderación, ya que incluso en el supuesto de que dicho interés legítimo exista, pueden prevalecer los intereses, derechos o libertades fundamentales del interesado que requieran la protección de sus datos personales, sobre todo cuando el interesado sea un niño (artículo 6. 1 f).

Cuando se trata de investigación impulsada por la Administración sanitaria o cualquier otra entidad pública, como es el caso de una Universidad o Instituto de Investigación de titularidadpública , o cuando la investigación revista "interés público" y se desarrolle en el ámbito de las administraciones públicas (artículo 6. 1. e), requiere el Reglamento que "los estados miembros fijarán los requisitos específicos a los que deberá atenerse dicha investigación (artículo 6. 2)". En cambio, la licitud del procesamiento de datos para la investigación por parte del sector privado se presta a interpretación, dado que dicha licitud se hace depender del "interés legítimo" del Responsable o del tercero cuyo alcance y requisitos no se definen (artículo 6. 1. f).

4.3. El tratamiento posterior de los datos con fines de investigación

El establecimiento de las condiciones para el uso secundario o posterior de los datos con fines de investigación fue objeto de un intenso debate durante la tramitación del Reglamento. La propuesta inicial de la Comisión prescindía de la necesidad de una nueva base legal para el tratamiento posterior con fines de investigación científica, siempre que dicho tratamiento

[31] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 abril 2014. Disponible en: http://www.dataprotection.ro/servlet/ViewDocument?id=1086.

no fuera incompatible con el fin para el que se recogieron inicialmente los datos[32].

Esta intelección resultaba enormemente favorable a la investigación médica y favorecía, por ejemplo, el uso de biobancos históricos de tejidos y muestras que podrían prescindir de recontactar con el interesado. En cambio, la enmienda del Parlamento suprimió dicho supuesto de uso secundario compatible, requiriendo una base legal nueva y específica para todo tipo de tratamiento posterior que no fuera el de garantizar la seguridad y el orden público y prevenir epidemias[33]. Con ello, se ponía en riesgo el consentimiento abierto contemplado entre otras en la normativa española reguladora de los biobancos. Finalmente, el Trilogue se decantó por una intelección favorable al uso secundario de datos para la investigación pero reforzando las garantías debidas al interesado (artículo 6. 4 y 89), erigiéndose en este punto la seudonimización como nuevo caballo de batalla entre el Parlamento, más garantista, y la Comisión, que pretendía favorecer al máximo la investigación[34].

Recuérdese que la Directiva derogada permitía el procesamiento posterior de los datos con fines distintos a los iniciales para los que fueron recabados en el caso de que los Estados miembros previeran garantías suficientes a dicho tratamiento secundario (Considerando 29). El nuevo Reglamento permite, en cambio, que los datos almacenados con determinado propósito inicial se destinen posteriormente a la investigación siempre que se respeten las garantías establecidas en el artículo 89 (Considerando 50). Así, el artículo 5. 1. b dice que: "… de acuerdo con el artículo 89. 1, el tratamiento ulterior

[32] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) C7-0025/12, art. 81, 82. Disponible en: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

[33] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), art. 81. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//EN.

[34] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation for trilogue - whole Regulation Brussels, 27 November 2015 (OR. en) 14481/15, art. 83. Disponible en: http://statewatch.org/news/2015/nov/eu-council-dp-reg-whole-text-14481-15.pdf.

de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerarán incompatibles con los fines iniciales". Según el artículo 89. 1 del Reglamento, el Responsable debe adoptar las medidas técnicas y organizativas suficientes para minimizar el uso de datos personales, comprendiendo entre las mismas, cuando sea posible sin comprometer el resultado de la investigación, medidas de seudonimización adecuadas.

Además, al objeto de determinar si la finalidad ulterior es compatible con el fin inicial para el que se recabó el consentimiento del interesado, siguiendo lo establecido en el artículo 6.4, el Responsable de los datos deberá tener en cuenta una serie de factores cumulativos como la relación entre los fines, el inicial y el posterior; el contexto en el que se hayan recogido los datos, atendiendo en particular a la relación entre los interesados y el Responsable del tratamiento; la naturaleza de los datos recabados; las consecuencias que pueden derivarse para los interesados; la existencia de garantías adecuadas, como por ejemplo, la seudonimización. Como referimos anteriormente, la definición de seudonimización finalmente adoptada por el Reglamento ha sido amplia, comprendiendo en la misma cualquier técnica presente o futura que impida que se llega a la re-identificación del interesado mediante un esfuerzo "razonable".

Al mismo tiempo, la norma contiene disposiciones adicionales referidas específicamente a la producción de nuevo conocimiento en materia sanitaria. El Considerando 53 provee que:

> "… El presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud… El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas".

Por otra parte, la investigación sobre salud es considerada en el Reglamento como un tipo específico de investigación científica (Considerando 159), al que por tanto deben aplicarse los mismos límites y garantías. Este debe ser el caso de los datos genéticos, biométricos y en general los relacionados con la salud de las personas cuya protección merece una concreción específica por parte del Derecho de los estados miembros.

Así, en el caso de investigación con datos sanitarios, el artículo 9 del RGPD requiere el aval del derecho estatal para su uso secundario no específi-

camente consentido[35]. Aunque dicho requerimiento parece salvado en el caso español, ya que la Ley Orgánica 3/2018 ha contemplado específicamente este uso secundario en el caso de la investigación sanitaria, como veremos más adelante.

4.4. Las garantías exigidas por el artículo 89 para el tratamiento de los datos dedicados a la investigación

El Reglamento consagra los derechos del interesado frente al tratamiento de sus datos, reforzando con algunos matices nuevos (como es el caso del derecho al olvido) el elenco de derechos ARCO contemplados en la Directiva anterior. No obstante, el nuevo artículo 89 permite la posibilidad de establecer limitaciones específicas al ejercicio de dichos derechos con objeto de favorecer la investigación científica e histórica, siempre que se adopten las garantías adecuadas para el tratamiento de los datos.

Así, el Reglamento permite a los Estados miembros establecer excepciones totales o parciales a los derechos de acceso, la rectificación, oposición y eliminación de los datos con el fin declarado de preservar la información que pueda ser valiosa para generar nuevo conocimiento de interés general. Con todo, dichas excepciones deben interpretarse de forma restrictiva, aplicándose solo aquellas que resulten "necesarias para alcanzar los fines"; y "sólo en la medida en que el ejercicio de los derechos citados imposibilite u obstaculice gravemente el logro de los fines científicos" (artículo 89. 2).

Por otra parte, el Reglamento autoriza específicamente a los Estados miembros a regular excepciones al derecho del interesado de oponerse al tratamiento de sus datos personales para la investigación cuando dicho procesamiento sea necesario "para el cumplimiento de una misión realizada por razones de interés público" (artículo 21. 6 y Considerando 45).

---

[35] Art. 9.1 Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y le tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, o datos relativos a la vida sexual o a las orientaciones sexuales de la persona física.
Art. 9.2 El apartado no será de aplicación cuando concurra alguna de las circunstancias siguientes: j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Además de la remisión anterior a la regulación de los Estados miembros, el propio Reglamento establece una serie de excepciones encaminadas a favorecer la investigación. Es el caso del artículo 17.3. d), el cual permite a los investigadores procesar determinados datos importantes para la integridad de la base de datos en la que se basa la investigación a pesar del interés manifestado por el afectado en la eliminación de dichos datos, siempre que dicha eliminación "pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos".

La nueva Ley Orgánica que interpreta la normativa europea se refiere específicamente a los citados aspectos como veremos posteriormente.

4.5. El deber de información y transparencia

A pesar de que para llevar a cabo proyectos de investigación científica con datos relativos a la salud no sea estrictamente necesario recabar el consentimiento del interesado cuando se trate de un uso secundario compatible con el consentimienro obtenido para el uso primario, o cuando se hayan seudonimizado los datos con las condiciones establecidas en el artículo 89 RGPD, incluso en estos supuestos, será necesario informar al interesado sobre el destino de sus datos "de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño" (artículo 12.1).

El artículo 13 del Reglamento regula el tipo de información que deberá facilitarse al interesado cuando los datos personales de salud o las muestras de las que se derivan dichos datos se obtengan directamente del interesado. En este caso para poder obtener el consentimiento se deberá informar sobre los siguientes extremos: identidad y datos de contacto del responsable, del delegado de protección de datos –sin que sea necesario identificarlo con nombre y apellidos–, fines del tratamiento a que se destinan los datos personales y base jurídica del tratamiento, los destinatarios de los datos –que pueden identificarse de forma genérica, refiriéndose a las categorías de destinatarios–, la transferencia de los datos a terceros, en su caso, los derechos que asisten al interesado en relación a sus datos, el periodo de conservación previsto, o cuando esto último no sea posible, los criterios utilizados para determinar dicho plazo. Además, según el propio artículo 13 en su apartado tercero, cuando el Responsable del tratamiento proyecte el tratamiento ulterior de datos personales con un fin distinto para el que solicita el consentimiento, el mismo Responsable proporcionará al interesado, con

anterioridad al tratamiento proyectado, información sobre ese otro fin y los derechos que asisten al titular de los datos.

A diferencia de lo que ocurría en la Directiva anterior, el Reglamento ofrece un marco más relajado, ya que al Responsable puede sortear la obligación de informar personalmente a los titulares cuando los datos no hayan sido obtenidos directamente del interesado si la comunicación personalizada de la información "resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de… investigación" (artículo 14. 5. b), aunque en tales casos, deberá el Responsable adoptar las medidas adecuadas para proteger los derechos y libertades e intereses legítimos de los interesados, "inclusive haciendo pública la información" (art. 14.5.b *in fine*).

4.6. Derecho de oposición

Se trata de un derecho de nuevo cuño consistente en solicitar que no se usen los datos personales en ficheros con fines de mercadotecnia y publicidad, o siempre que exista una razón legítima y fundada para oponernos al tratamiento para cualquier otra finalidad cuando no se haya prestado previo consentimiento por escrito.

El Reglamento excepciona este derecho de oposición en el caso de que el tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público. El Considerando 54 ejemplifica dichas razones, sin contemplar la investigación científica como tal dentro de las excepciones:

> "El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.o 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines."

Así, el artículo 21 del Reglamento especifíca en su apartado 6 que "cuando los datos personales se traten con fines de investigación científica de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan". Se entiende que dicho derecho sigue vigente incluso en el caso de que los datos hayan sido seudonomizados, puesto que siguen siendo datos personales sobre los que existe una trazabilidad y posibilidad de reidentificación posterior.

4.7. La prohibición del perfilado a partir del uso secundario de datos para la investigación

Otro aspecto que interesa destacar en relación al tratamiento posterior de los datos es el relativo a la prohibición del perfilado. La Directiva derogada establecía que "el tratamiento ulterior de datos personales con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona" (Considerando 29).

El G29, por su parte, en su Opinión sobre la interpretación de la limitación del fin, consideró que la expresión "medidas o decisiones" debía interpretarse en sentido extenso, de forma que alcanzara cualquier decisión que impactara de forma significativa en los interesados tanto positiva como negativamente[36].

El Reglamento no recoge dicha prohibición con el fin declarado de permitir el tratamiento derivado o secundario de datos para la investigación que tenga un impacto de cualquier tipo en los interesados. No obstante, el nuevo texto legal obliga a adoptar medidas para prevenir dicho resultado. El artículo 35 (3) (a) ordena que la evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de que,

> "La evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos

[36] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 de abril de 2013. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

jurídicos para las personas físicas o que les afecten significativamente de modo similar".

A su vez, el artículo 22.1 prohíbe a los Responsables del tratamiento de datos sensibles que tomen una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

Por tanto, a pesar de que el Reglamento elimina la prohibición de desarrollar una investigación basada en el tratamiento secundario de datos que pueda tener un impacto de cualquier tipo en los interesados, en su lugar, introduce importantes garantías para evitar que dicho resultado se produzca. En caso de que los Responsables del tratamiento no realicen una EIPD, pueden encontrarse con la prohibición de llevar a cabo la investigación que comprometa decisiones basadas en los datos personales de los interesados.

La elaboración de perfiles plantea retos específicos en el ámbito de la salud[37]. En el Reglamento se establecen restricciones específicas para evitar el riesgo del perfilado con el objeto de evaluar la salud de una persona física identificada o identificable, siendo necesario en estos casos evaluar el riesgo antes de iniciar el procedimiento, salvo en el caso de que el perfilado se haga por parte de un profesional de la medicina sujeto a secreto profesional, en cuyo caso la evaluación de impacto no será necesaria; restricción que parece una clara concesión a los servicios de salud.

Tras repasar las principales novedades contenidas en el nuevo Reglamento europeo, a continuación veremos cuál ha sido el desarrollo que de los principios y mecanismos procedimentales establecidos en el RGPD ha hecho el legislador español en materia de datos genéticos y de salud, especialmente, en lo que hace a su uso para generar nuevo conocimiento.

5. Marco legal para el uso de datos en investigación sanitaria y biomédica en la Ley Orgánica 3/2018

Hemos dicho ya que, a partir de la delegación operada en el Reglamento, la investigación en salud y la investigación biomédica han merecido un tratamiento señalado en la nueva Ley española de protección de datos. Se

[37] Serrano Pérez, M. M., *"Big Data o la acumulación de masiva de datos sanitarios: derechos en riesgo en el marco de la sociedad digital", Revista Derecho y Salud, Vol. 25. Extraordinario XXIV Congreso 2015,* pp. 51-64.

trata posiblemente del ámbito en el que el legislador español ha desplegado más decididamente la potestad reguladora concedida por el Reglamento, desarrollando de forma posibilista las previsiones contempladas en el mismo. Téngase en cuenta que hasta la promulgación de la nueva Ley Orgánica, carecíamos de un estatuto marco de la investigación sanitaria o biomédica en España[38]. Ninguna de las leyes vigentes en materia de sanidad o de investigación contemplaba dicho estatuto[39].

---

[38] Tal como señala Pilar Nicolas, hasta la promulgación de la Ley Orgánica 3/2018, el uso de datos sanitarios y genéticos en la investigación adolecía de una regulación fragmentaria e incompleta. Vid. Nicolás Jiménez, Pilar, "Investigación biomédica y bigdata sanitarios", *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Coord.), Ed. Thomson Reuters, Cizur Menor, España, 2019 (en prensa).

[39] La Ley de Investigación Biomédica, y su normativa de desarrollo (Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica) se refiere exclusivamente a la utilización de datos asociados a las muestras biológicas. La regulación de la historia clínica del artículo 16 de la Ley 41/2002, de Autonomía del Paciente, contempla la legitimidad de su uso con fines de investigación mediante remisión a la normativa de protección de datos, pero en términos confusos cuya interpretación no es unánime. No quedaba, por tanto, resuelto de manera nítida si el consentimiento del sujeto es imprescindible cuando los datos se van a utilizar de manera disociada, ni quién o como se está legitimado para acceder a la historia clínica con fines que no sean asistenciales. Era preciso acudir a la normativa general sobre protección de datos para identificar las figuras con título habilitante a estos efectos, lo cual requería esfuerzos interpretativos, y suponía soluciones que poco homogéneas y, posiblemente, insatisfactorias. Pero ni siquiera resolver estos dilemas supondría una solución definitiva puesto que ha de tenerse en cuenta que, aunque la historia clínica es una fuente valiosísima de información sobre la salud de los individuos, de gran utilidad potencial para la investigación, no es la única, de manera que, cualquier solución que pueda derivarse de esta Ley, sería sectorial. Piénsese en otros archivos como los registros de enfermedades o los que almacenan resultados de análisis poblacionales o las bases de datos donde se depositan los resultados de proyectos de investigación. La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud que se refiere al intercambio electrónico de información clínica entre las Comunidades Autónomas, pero únicamente con el objetivo de mejorar la calidad de la asistencia a los pacientes, en el marco de su objeto, no se refiere a la investigación sanitaria como tal. Tampoco la contemplaba hasta ahora, la Ley 33/2011, de 4 octubre, General de Salud Pública, que contenía revisiones relativas al acceso a datos de salud de los ciudadanos, pero únicamente en relación a estudios encaminados a la prevención de riesgos graves para la salud de la población. En cuanto a la normativa relativa al desarrollo de ensayos clínicos contiene referencias al tratamiento de los datos pero únicamente para esta modalidad de investigación biomédica, y lo mismo ocurre con el *Código Tipo de protección de datos personales en el ámbito de la investigación clínica*, de Farmaindustria, del año 2009. Farmaindustria, *Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la Farmacovigilancia*, 1/1/2004. Disponible en: http://

5.1. Habilitación legal que salva el marco normativo vigente

Siguiendo el principio básico establecido en el artículo 9.2 del Reglamento en relación a las categorías especiales de datos, el artículo homónimo de la LOPDGDD establece una prohibición general de tratar los datos relativos a la salud, salvo en determinados supuestos. De entre éstos, el propio artículo 9 establece que los contemplados en las letras g), h) e i), (tratamiento necesario por razones de interés público, tratamiento necesario para fines de medicina preventiva o laboral, diagnóstico médico y prestación de asistencia sanitaria; tratamientos necesarios para garantizar la salud pública, así como la calidad y seguridad de la asistencia sanitaria), deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad, añadiendo que:

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

Se trata de una habilitación importante a la hora de fijar el rango normativo en materia de regulación de los tratamientos de datos sanitarios, ya que, a partir de los criterios establecidos en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, el marco actual se ha desarrollado a través de leyes ordinarias, como es el caso de la Ley General de Sanidad, entre otras. Este rango de ley ordinaria seguirá, por tanto, siendo suficiente para desplegar el uso de los datos de salud y asociados a la actividad sanitaria. Así, la Disposición Adicional17ª de la LO 3/2018, intitulada "Tratamiento de datos de salud", salva en su apartado primero las habilitaciones legales actualmente existentes como base del tratamiento de datos sanitarios[40].

www.farmaindustria.es/web/documento/codigo-tipo-de-farmaindustria-de-proteccion-de-datos-personales-en-el-ambito-de-la-investigacion-clinica-y-de-la-farmacovigilancia-2/

[40] Disposición adicional decimoséptima. Tratamientos de datos de salud. 1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo: a) La Ley 14/1986, de 25 de abril, General de Sanidad. b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.f) La Ley 14/2007, de 3 de julio, de Investigación biomédica. g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.i) El texto refundido de la Ley

Es por tanto fundamentalmente conservadora la posición de la nueva Ley Orgánica 3/2018 en materia de protección de datos sanitarios o relativos a la salud, aunque existen algunas pocas pero importantes novedades al respecto[41]. Así, como veremos, el tratamiento de datos sanitarios con fines de investigación biomédica se regula en la propia LOPDGDD, fijándose el rango orgánico para su regulación y modificación futura.

Por otra parte, ni los Comités de Ética de la Investigación ni otros comités o instituciones involucrados en el control de la actividad biomédica, tenían atribuidas en la legislación española competencias para evaluar los proyectos de investigación con datos[42]. Algunos Comités ejercían de hecho esa función pero no existen procedimientos reglados ni todos los investigadores solicitan la revisión[43]. La única referencia normativa vinculante al control o autorización de esta investigación se encuentra en el artículo 58.2 de la Ley 14/2007, de Investigación Biomédica (LIB) cuando recoge la posibilidad de autorización por parte de la Autoridad competente en materia de protección de datos para la utilización de ciertos datos en supuestos muy concretos.

La nueva ley española de protección de datos ha venido, por tanto, a llenar un vacío importante en materia de investigación con datos sanitarios. Preciso es constatar sin embargo que el proyecto de ley orgánica incialmente presentado a las Cortes carecía de previsiones específicas en relación a la

---

de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio. j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

41 Martinez Rojas, Ángela, "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* Núm. 42, 2016.

42 La única excepción es la normativa específica que regula los estudios observacionales con medicamentos. La Orden SAS/3470/2009, de 16 de diciembre, por la que se publican las directrices sobre estudios posautorización de tipo observacional para medicamentos de uso humano, especifica que los estudios observacionales en los que se recoge información sobre medicamentos que se realizan con datos ya existentes que no contengan información de carácter personal, no requieren ni consentimiento del sujeto ni la aprobación por un Comité Ético de Investigación Clínica (CEIC) acreditado o Comité de Ética de la Investigación, en su caso.

43 No obstante, el RD 1090/2015 establece que la investigación clínica debe desarrollarse en un entorno que garantice la protección de las personas que participan en ella y en consonancia con elementos como la Declaración de Helsinki, aprobada por la Asociación Médica Mundial, y el Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, suscrito en Oviedo. Además las editoriales exigen la aprobacion de un CEI como requisito para la publicacion de los resultados de los proyectos, independendientemente de que sean obsercacionales con datos, u otro tipo de proyecto.

investigación sanitaria[44]. En efecto, la regulación finalmente aprobada trae causa de la preocupación manifestada por numerosos colectivos científicos y sanitarios, que dieron lugar a comunicados públicos y a reuniones con la Agencia Española de Protección de Datos, en un inicio, y posteriormente, a la presentación de enmiendas durante la tramitación de la Ley por parte de varios grupos parlamentarios. Siendo el tratamiento de datos la base para poder desarrollar proyectos de investigación en materia de salud y biomedicina, existía el temor fundado de que el legislador ignorara la oportunidad abierta por la nueva normativa del RGPD para postergar de nuevo el establecimiento de un marco legal de la investigación sanitaria. Finalmente, en la tramitación parlamentaria la LOPDGDD se dotó de una serie de previsiones al objeto de garantizar el adecuado desarrollo de la investigación en materia de salud y biomedicina, preservando la protección del derecho fundamental a la protección de datos.

Desde el punto de vista de técnica legislativa es también obligado constatar que con dudosa técnica legislativa, la Ley Orgánica 3/2018 ha optado por ubicar el título habilitante general para la investigación biomédica en sede de la Ley General de Sanidad, añadiendo un nuevo capítulo II al título VI, intitulado "Tratamiento de datos de la investigación en salud". El artículo 105 bis del nuevo capítulo establece que "El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Ley Orgánica de Protección de Datos Personales y de Garantía de los Derechos Digitales". Es cierto que el régimen general de la investigación biomédica y sanitaria podría haberse integrado en la LIB, el cual parece un instrumento más específico en materia de investigación; sin embargo, se ha optado por la Ley General de Sanidad, quizá por considerarla más comprensiva en cuanto a la mayor extensión de su ámbito de aplicación, referido a cualquier tipo de dato o actividad sanitaria. Sin embargo, la regulación efectiva del nuevo marco normativo de la investigación sanitaria con datos de salud no se desarrolla en la propia LGS; el nuevo artículo 105 bis de la Ley General de Sanidad remite a la regulación establecida en la Disposición Adicional 17ª de la nueva Ley Orgánica de Protección de Datos, operándose así una remisión cruzada que termina residenciando la regulación de la investigación con datos sanitarios en la propia Ley Orgánica.

Como resultado de todo ello y a diferencia de lo que ocurre en el tratamiento de datos de salud con fines asistenciales, que podrá seguir siendo

[44] 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. BOCG, Serie A: Proyectos de Ley 24 de noviembre de 2017 Núm. 13-1. Disponible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

desarrollado por ley ordinaria, el legislador ha querido congelar el rango normativo del marco general para el uso de datos médicos en investigación, estableciendo una diferencia significativa entre ambos tipos de finalidad, asistencial y de investigación. Como resultado de esta opción legislativa se enmarca la investigación científica en un régimen normativo de carácter excepcional en comparación con su uso asistencial o administrativo, que puede seguir siendo regulados por ley ordinaria.

La doctrina ha criticado esta opción legislativa en el sentido de que "sistemáticamente hubiera sido más oportuno que el tratamiento de datos en investigación en salud hubiera constituido un nuevo título en la LIB, como norma que de manera más global regula la investigación biomédica"[45].

5.2. La regulación del consentimiento

En cuanto al régimen efectivamente establecido para el uso de datos sanitarios en investigación, se ha dicho que las novedades introducidas revisten un carácter más procedimental que de fondo[46]. Sin embargo, entendemos que la LOPDGDD hace algo más que esto. Así, el Preámbulo de la nueva Ley señala que:

> "El Reglamento general de protección de datos no afecta a dichas habilitaciones (se refiere, entre otras, al uso de datos de salud en investigación), que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos".

En efecto, haciendo uso de la habilitación del Reglamento, la Ley española establece un régimen excepcional en materia de investigación sanitaria en atención a la importancia social y económica de dicha actividad ciéntifica. Según lo establecido en la DA 17.2 que regula el tratamiento de datos en la

---

45 Nicolás Jiménez, Pilar, "Investigación biomédica y bigdata sanitarios", *op. cit.*.

46 Martinez Rojas, Ángela, "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea". *Revista Aranzadi de Derecho y Nuevas Tecnologías,* Núm. 42, 2016. Morales Barcelo, Judith, "Big data y protección de datos: especial referencia al consentimiento del afectado", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* Núm. 44, 2017, p.16.

investigación en salud, no se requiere el consentimiento cuando no sea posible la identificación de la persona por haber sido seudonimizados sus datos, situaciones de excepcional gravedad para la salud pública, o cuando se trate de estudios relacionados con el área de investigación para la que ya se obtuvo consentimiento. Todo ello siempre que se cumplan determinados requisitos y condiciones adicionales orientadas a proteger el interés del paciente y evitar los efectos adversos y la posible discriminación que pudiera derivarse de un uso inconsentido y abusivo de dicha base legal para el tratamiento.

5.3. El consentimiento genérico

En primer lugar, a partir de la autorización recogida en el Reglamento General de Protección de Datos, la Ley española desarrolla una regulación flexible del alcance que puede darse al consentimiento del interesado, superando la interpretación más restrictiva contenida en el artículo 60 de la LIB.[47] Teniendo en cuenta la interpretación derivada directamente del RGPD, la DA 17.2. letra a) de la nueva Ley señala que no será necesario que la persona preste su consentimiento para una investigación o rama concreta, sino que, será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, añadiendo que: *"[…] Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora"* (DA 17ª 2.a, *in fine*)[48].

En segundo lugar, la letra b) de la disposición citada contempla el supuesto específico de las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública. Este tipo de autoridades podrán acometer ellas mismas, o a través de los equipos de investigación

[47] El Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para la investigación biomédica, advierte que las previsiones relativas a la utilización de las muestras biológicas son aplicables a los datos asociados. Así, por ejemplo, cuando un investigador solicita a un biobanco la cesión de muestras, se revisará por un mismo procedimiento si se debe autorizar esta cesión y también la de los datos del sujeto fuente que estuvieran asociados a la misma. El tratamiento de los datos quedará por tanto sujeta a la LIB y al RD 1716/2011 en tanto acompañen al material biológico.

[48] Esta intelección ha sido corroborada por la Agencia Española de Protección de Datos según la cual, "será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, como por ejemplo, la investigación oncológica, o incluso para ámbitos más extensos". Agencia Española de Protección de Datos. Informe: 073667/2018 https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

asociados, "estudios científicos", se entiende que haciendo uso de datos de salud, sin el consentimiento de los afectados, "en situaciones de excepcional relevancia y gravedad para la salud pública".

Tanto la gravedad como la relevancia en relación a la salud pública son conceptos jurídicos indeterminados que cuentan, sobre todo en el caso de la primera, con una interpretación jurisprudencial que permite definir más claramente su perímetro. No obstante, es preciso advertir que ambas circunstancias deben ser interpretadas de forma restrictiva por constituir regímenes de excepcionalidad en relación al tratamiento de los datos personales. En este sentido, deberá entenderse que el consentimiento será exigible siempre que se pueda obtener sin menoscabo de la eficicacia del estudio dirigido a responder a una situación de especial relevancia o gravedad.

5.4. Reutilización de datos de salud para la investigación biomédica

La letra *c)* de la DA 17.2 considera que es "lícita y compatible" (con la finalidad inicial para la que se recabó el consentimiento, se entiende) la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, "habiendóse obtenido al consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial". No se requiere, por tanto, volver a recabar el consentimiento del sujeto fuente en el caso de que se reutilicen datos para una investigación "relacionada con en la que se integrase científicamente el estudio inicial" (DA 17. 2. c), siempre y cuando se cumplan unas garantías mínimas, como atender al deber de información y transparencia y obtener informe favorable previo del Comité de Ética de la Investigación (CEI).

Nótese que el informe del CEI deberá valorar si las áreas de investigación para las que se solicita autorización están efectivamente relacionadas con el área en la que se integraba o a la que pertenecía científicamente el estudio inicial. Es evidente que dicha apreciación puede dar lugar a opiniones dispares y que requerirá, más pronto o más tarde, de unas directrices emanadas de la Comisión Europea de Protección de Datos que permitan armonizar las interpretaciones en relación al alcance del uso posterior consistente en los diversos países de la Unión.

La misma regla de autorización de uso secundario es aplicable también para aquellas investigaciones iniciadas con anterioridad a la entrada en vigor de la Ley. Según la Disposición Transitoria sexta:

> "Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:[…] b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial".

A pesar de que la citada DT no lo menciona, entendemos que también en este caso se requiere informe favorable previo del comité de ética de la investigación al tratarse de un supuesto similar al contemplado en la DA.

En el caso de la reutilización de datos personales contemplado en la DA 17ª 2.c) se prevé además que:

> "[…] los Responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato".

Se trata de una concreción del deber de información y transparencia contenido en el artículo 13 del Reglamento citado en la medida en que permite al interesado conocer el uso posterior que se está dando a sus datos sanitarios y, en el caso de que no desee autorizar dicho uso, le permitir hacer uso de su derecho de oposición. Entendemos que dicho derecho no decae cuando se emplean datos nominativos para usos secundarios o posteriores sin el consentimiento del interesado, ya que las excepciones contempladas al derecho de oposición en la letra *e)* de la misma disposición (DA 17ª.2) se refieren, como veremos, a tres supuestos ajenos al presente, que además, han de ser interpretados restrictivamente por tratarse de excepciones a derechos reconocidos.

5.5. Investigación a partir de datos seudonimizados

La letra *d)* de la DA 17ª 2 considera lícito el uso de datos personales seudonimizados con fines de investigación en salud, y, en particular, de investigación biomédica. La correcta intelección de dicha letra supone extender el

régimen excepcional permitido por los artículos 9 y 89 del Reglamento a los datos seudonimizados, siempre que se cumplan determinadas condiciones en el tratamiento de dichos datos. Por tanto, entendemos que este precepto permite prescindir del consentimiento para el uso posterior de datos siempre que previamente se haya procedido a su seudonimización de acuerdo con determinados estándares a los que alude la norma.

En nuestra opinión, la misma regla debería regir en los supuestos en los que se autorice el tratamiento de muestras biológicas codificadas, conforme al artículo 58.2 de la Ley 14/2007, siempre que existan medidas técnicas adecuadas que impidan la reidentificación del sujeto fuente[49].

En cambio, entendemos que por su especial sensibilidad, cuando la información a utilizar contenga datos genéticos y se pretenda emplearlos en investigación sin el consentimiento expreso del interesado, se requerirán medidas específicas de seguridad para evitar la reidentificación del sujeto fuente tal como prevé el apartado ii) de la DA 17.2.d.2º. Este es, en nuestra opinión el sentido del Considerando 53 del Reglamento el cual prevé como sabemos que, a pesar de que "el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud… El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas".

Hasta aquí nos hemos referido a la reutilización de los datos sanitarios con fines de investigación para proyectos concretos, la cual podrá llevarse a cabo sin volver a solicitar el consentimiento del interesado siempre que se proceda a la seudonimización de los datos. Es claro que el supuesto se refiere al uso de los datos una vez seudononimizados, pero, podemos preguntarnos si se requiere consentimiento previo para poder proceder a seudonimizar las historias clínicas con la intención de ponerlas a disposición de los investigadores en el futuro.

En España existen varios programas públicos que ofrecen plataformas de datos seudonimizados a los investigadores, como es el caso del PADRIS en Cataluña, gestionado mediante encomienda de gestión por la entidad pública de derecho privado AQUAS[50]; o el proyecto de puesta a disposición de copias

[49] En este sentido se pronuncia la Agencia Española de Protección de Datos, Informe 073667/2018. https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf.

[50] Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS). Disponible en: http://aquas.gencat.cat/ca/inici

espejo de los historiales clínicos electrónicos gestionados por el Ente Público *Osakidetza-Servicio vasco de salud*. En ambos casos, cabe preguntarse si se requiere o no la autorización del interesado para seudonimizar su historial o parte del mismo sin que se sepa aún con certeza para qué tipo de proyectos de investigación se emplearán dichos datos.

Se ha dicho más arriba que la seudonimización, como antes la anonimización, constituye en el nuevo Reglamento un caso de tratamiento posterior, al que le son aplicables las premisas de limitación del fin previstas en el propio Reglamento. Serían, por tanto, aplicables los requerimientos establecidos para el uso y tratamiento posterior de datos sensibles que recoge el propio Reglamento, incluida la obligación de informar a la que alude el artículo 14 del RGPD cuando se refiere a los datos que no hayan sido directamente obtenidos del interesado. En este sentido, a pesar de la omisión de la LOPDGDD, entendemos que debe integrarse dicha laguna aplicando directamente el Reglamento al obligar al encargado del tratamiento a proporcionar información al interesado sobre la seudonimización de los datos personales que obran en su historia clínica con la intención de poner a disposición de los investigadores los indicadores relevantes procedentes de la misma.

Por lo dicho, entendemos que el sentido del segundo párrafo de la letra *c* (DA 17ª 2), el cual obliga a informar sobre este hecho por medios electrónicos, supone que los Responsables de los datos cumplen con informar sobre dicho procedimiento, permitiendo, como se ha dicho en el epígrafe anterior, que el interesado se oponga a que sus datos sean objeto de seudonimización mediante una cláusula *opting out*. El derecho a oponerse debería estar claramente indicado en la hoja informativa, ser fácil de ejercitar y no debería suponer coste alguno para el interesado.

5.6. Garantías técnicas para los tratamientos de datos de salud en investigación

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá, según la misma letra *d* de la DA 17.2, de varios requisitos técnicos:

> "1º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. 2º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. ii)

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

A estas previsiones deben añadirse las contenidas en la letra *f)* del mismo precepto que también se refiere a los requisitos técnicos que debe reunir la investigación con datos sanitarios en particular la que opera con datos seudonimizados. Dicha letra *f* dispone que el Responsable del tratamiento deba asegurarse de que se cumplan los siguientes requisitos basados en el principio de minimización de datos:

> "1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos. 2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. 3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados. 4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679".

La letra transcrita es producto de una enmienda que a falta de una integración sistemática correcta en la norma, produce problemas de interpretación importantes. Como puede verse, a pesar de contener previsiones aplicables a todo proyecto de investigación en salud pública o biomédica, varios de sus preceptos se refieren de forma específica al tratamiento de datos seudonimizados. Se hace precisa, por tanto, la interpretación integradora de las letras *d)* y *f)* de la DA 17.2 en relación a la investigación con datos personales seudonimizados. Es el caso, por ejemplo, de los números 1º y 3º de las letras d) y f), respectivamente. El primero requiere que se opere una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonomización y conserven la identificación que posibilite la reidentificación. El número 3 de la letra f exige que se adopten medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

En un intento de interpretación integradora, parece que en relación a los requisitos técnicos y funcionales referidos a los datos seudonimizados, podríamos concluir que son los siguientes:

- Separación técnica y funcional entre el investigador y el que realiza la seudonimización. Es importante reforzar esta idea, ya que aún no está del todo desterrada la costumbre de algunos médicos de seudonomizar o codificar ellos mismos la información que obra en los historiales médicos custodiados para destinarlos a la investigación. En todo caso, deberán adoptarse todas las medidas necesarias para que los investigadores no puedan acceder a los códigos de identificación de los interesados.

- En el caso de que se requiera evaluación de impacto según la lista elaborada por las autoridades de control y en todo caso cuando se trate de tratamiento de datos a gran escala, será necesario evaluar los riesgos referidos a la posibilidad de reidentificación.

- En todo caso deberán adoptarse medidas técnicas específicas para evitar la reidentificación tanto por parte de los investigadores como por parte de terceros.

- Firma de un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación por parte de los investigadores.

- e deberán observar las normas de calidad y buenas prácticas establecidas en los códigos del sector.

No obstante, la Ley prevé una excepción a la prohibición de reidentificación cuando se produzca un hallazgo inesperado (*incidental finding) al* trabajar con datos seudonimizados o codificados, ya que podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria (DA 17ª. 2. d. *in fine*).

5.7. Excepciones a los derechos ARCO

La Disposición adicional 17ª prevé excepciones al ejercicio de los derechos de acceso, rectificación, limitación y oposición cuando se produzcan las circunstancias previstas en el artículo 89.2 del Reglamento, es decir, "*siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines"*.

En concreto, la citada DA 17ª .2.e se refiere a tres supuestos en los que dichos derechos podrán excepcionarse:

> "1.º Cuando los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley".

Nótese que los tres supuestos son ajenos a la previsión de la letra c de la DA17.2, en la que se contempla la reutilización de datos personales sin consentimiento con fines de investigación afin a la incial. En este último caso, el legislador quiere que se informe al interesado que podrá oponerse al uso de los datos para la investigación proyectada o en marcha, y ejercer otros derechos como la cancelación o la rectificación.

En nuestra opinión, tampoco debería excepcionarse el derecho del interesado oponerse a la seudonimización de los historiales clínicos con fines de investigación que se ejerce ante el responsable de dicho tratamiento de seudonimización puesto que se trata de un derecho previo que no obstaculiza gravemente el logro de los fines científicos que se pueden lograr con el resto de los datos seudonimizados puestos a disposición del investigador. En este caso, bastará con informar al interesado de forma directa o través de la página web de que se trate de que se vaya a proceder al tratamiento de los datos obrantes en su historial si no existe oposición por su parte.

5.8. Control ético de la investigación sanitaria

Los tratamientos secundarios de datos en investigación sanitaria requerirán, según lo previsto en la Disposición Adicional 17ª de la LOPDGDD, el informe previo favorable del Comité de Ética de la Investigación (CEI). En este caso, el CEI deberá asegurarse que el alcance del consentimiento inicialmente prestado por el sujeto fuente o el interesado para determinada investigación, es compatible con el uso posterior de dichos datos para "finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial" (DA 17ª 2. c).

La intervención del CEI será asi mismo preceptiva en el caso de proyectos de investigación que requieran reutilizar datos personales recogidos con anterioridad a la entrada en vigor de la Ley Orgánica 13/2008 (DT 6ª).

También requerirán dicho informe favorable del CEI los proyectos de investigación que hagan uso de datos seudonimizados e incluso, anonimizados, "según lo dispuesto en la normativa sectorial" (DA 17ª.2.g). Convendría, en todo caso, que se tratarse de un procedimiento abreviado, incluso de una mera notificación para comprobar que no existe riesgo de reidentificación.

No se menciona en la nueva ley la revisión por parte del CEI del tratamiento de datos codificados, en los que los investigadores cuentan con ficheros identificadores de los sujetos, pero no hay que excluirla teniendo en cuenta lo previsto en los códigos éticos como el de CIOMS o los principios éticos de la Declaración de Helsinki y las normas internacionales de calidad y sobre buena práctica clínica entendidas en sentido amplio[51].

En relación a la composición de los CEI, la ley prevé que en el plazo máximo de un año desde la entrada en vigor de la LOPDGDD, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados. (DA 17ª 2.h). En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

6. Anexo. Ruta básica de control de los proyectos de investigación sanitaria y biomédica que impliquen tratamiento masivo de datos

A continuación, se despliega el check list básico de los ítems que deben comprobar el Responsable o Encargado del tratamiento, el Delegado de Protección de Datos, el CEI del centro a través del Informe Previo cuando se proceda a la seudonimización de los historiales clínicos para la investigación.

[51] Beranger, Jérôme, "La valeur éthique des Big data en santé", *Les Cahiers du Numerique*, Núm. 1, Vol. 12, 2016, pp. 109-132.

Comprobación de la base legítima para el tratamiento de los datos
Elaboración de evaluacion de impacto
Plan de proteccion de datos
Medidas de seguridad
Plan de contingencia en caso de quiebras o fugas
Registro de actividad
Consulta previa a la autoridad de control en el caso de que haya un riesgo alto resultante de la EIPD.
Métodos para la recogida de datos, principio de minimización ("adecuado, pertinente y limitado a lo necesario").
Procesos de anonimización y/o seudonimización
Cesión de datos con fines de investigación
Participantes son informados de seudonimización y la puesta a disposición a través de página web
Se garantizan los derechos ARCO que no resulten excepcionados con motivación
Articulación de mecanismos de oposición a la seudonimización y puesta a disposición
Publicación de los resultados de investigación
Información sobre quiebras o fugas, en su caso

7. Bibliografía

Abiduzzaman, M. *et ál.,* "Big data in healthcare –the promises, challenges and opportunities from a research perspective: a case study with a model database", *AMIA. Annual Symposium proceedings*, AMIA Symposium, 2017.

Aced Félez, Emilio, "Protección de Datos y Transformación Digital en Sanidad", *Revista de la sociedad española de informática y salud*, Vol. 118, 2016.

Agencia Española de Protección Datos. *Carácter de dato personal de la dirección IP.* Informe 327/2003.

Agencia Española de Protección Datos. *Guía para la Evaluación de Impacto en la Protección de Datos Personales que sirve de referencia en materia de requisitos técnicos y procedimentales que debe reunir una EIPD*.

Agencia Española de Protección Datos, *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD*, 2016.

Agencia Española de Protección Datos, Informe 073667/2018.

Agencia Española de Protección Datos, Informe: 073667/2018.

Alhadeff, J. / Van Alsenoy, B. / Dumortier, J., "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions", *Managing Privacy through Accountability*, Guagnin, D. / Hempel, L. / Ilten, C.

/ Kroener, I. / Neyland, D. / Postigo, H. (Eds), Palgrave Macmillan, Londres, Reino Unido, 2012.

Andreu Martínez, Mª Belén / Pardo López, Mª Magnolia / Alarcón Sevilla, Verónica, "Hacia un nuevo uso de los datos de salud", *Ius et Scientia,* Núm. 1*,* Vol. 3, 2017.

article 29 data protection working party*, Guidelines on Data Protection Officers ('DPOs')* 243 /2016, Adopted on 13 December 2016, last Revised and Adopted on 5 April 2017.

article 29 data protection working party, *Guidelines on Data Protection Officers ('DPOs')*, Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017.

article 29 data protection working party, *Opinion 03/2013 on purpose limitation*, 2 de abril de 2013.

article 29 data protection working party, *Opinion 05/2014 on Anonymisation Techniques*, Adopted on 10 April 2014.

article 29 data protection working party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 abril 2014.

article 29 data protection working party, *Statement of the WP29 on the impact of the development of Bigdata on the protection of individuals with regard to the processing of their personal data in the EU* WP 221, 14/EN, Adopted on 16 September 2014.

Beranger, Jérôme, "La valeur éthique des Big data en santé", *Les Cahiers du Numerique*, Núm. 1, Vol. 12, 2016.

CEAB, *Controles éticos en la actividad biomédica. Análisis de situación y recomendaciones*, Instituto Roche, 2009.

Chico, V., "The impact of the General Data Protection Regulation on health research", *British Medical Bulletin*, Núm. 1, Vol. 128, 2018.

Debiès, Elise, "Apertura de datos de salud en francia, impacto en la investigación y la seguridad social", *Bioderecho.es*, Núm. 5, 2017.

Elger, Bernice S. / Caplan, Arthur L., *Consent and anonymization in research involving biobanks*, EMBO Reports, 2006.

Farmaindustria, *Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la Farmacovigilancia*, 1/1/2004.

Gonzalez, P., "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata*, Núm. 24, 2017.

Jiménez Asensio, Rafael, *Introducción al nuevo marco normativo de la protección de datos personales en el sector público,* IVAP, Oñati, España, 2019.

Masse, Estelle, *General Data Protection Regulation – what tidings do ye bring?,* 21 December 2015.

Moerel, Lokke / Prins, Corien, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, May 25, 2016.

Mostert, Menno / Bredenoord, Annelien L. / Van Der Slootb, Bart / Van Deldena, Johannes J.M. "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", *European Journal of health law*, Vol. 25, 2018.

Morales Barcelo, Judith, "Big data y protección de datos: especial referencia al consentimiento del afectado", *Revista Aranzadi de Derecho y Nuevas Tecnologías* Núm. 44, 2017.

Nicolás Jiménez, Pilar, "Investigación biomédica y bigdata sanitarios", *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Coord.), Ed. Thomson Reuters, Cizur Menor, España, 2019.

Nordforsk, Ethical review, data protection and biomedical research in the nordic countries: a legal perspective, Policy Paper, 1/217.

Reichel, Jane, "Oversight of EU medical data transfers – an administrative law perspective on cross-border biomedical research administration", *Health Technol.* Vol. 7, 2017.

Riaño Galán, Teresa, "Investigación biomédica, tratamiento de muestras biológicas humanas y iobancos", *Rev. Bioderecho.es*, Vol. 1, 2014.

Serrano Pérez, M. Mercedes, "Big Data o la acumulación de masiva de datos sanitarios: derechos en riesgo en el marco de la sociedad digital", *Revista Derecho y Salud*, Vol. 25. Extraordinario XXIV Congreso 2015.

Tene, Omar / Polonetsky, Jules, "Beyond IRBs: Ethical Guidelines for Data Research", 72 *Wash. & Lee L. Rev. Online* 458, 2016.

Pruebas genéticas en los tratamientos de reproduccion asistida, con especial referencia a los tests de portadores y *matching* genético. Controversias en materia de información*

Genetic tests in assisted reproduction treatments, with special reference to carrier tests and genetic matching. Controversies in the field of information

Dr. Fernando Abellán-García Sánchez

Doctor en medicina legal por la Universidad Complutense de Madrid

Asesor jurídico de la Sociedad Española de Fertilidad (Madrid, España)

DOI: 10.14679/1140

Sumario: 1. Introducción. Tipología de los estudios genéticos en la medicina reproductiva. 2. Estudios genéticos con fines clínicos a pacientes y donantes de gametos. 2.1. Contexto normativo de las pruebas genéticas a pacientes y donantes de gametos. 2.2. Lo que dice la normativa en cuanto a las pruebas genéticas a realizar. 3. Un paso de gigante en la obtención de información: el análisis de portadores y el *matching* genético. 3.1. ¿En qué consisten estas pruebas? Los conceptos de alto y bajo riesgo genético y de riesgo residual. 3.2. Problemas de información en torno a los tests de portadores y el *matching* genético. 4. Conclusiones.

Resumen / Abstract: Tras describir la tipología de las pruebas genéticas que se desarrollan en la medicina reproductiva el trabajo se centra en las particularidades de los tests genéticos de portadores y el *matching* genético, para razonar, aportando

* Artículo recibido el 14 de julio de 2019 y aceptado para su publicación el 22 de julio de 2019.

ejemplos, por qué el marco legal vigente resulta insuficiente para dar respuesta a las controversias que se plantean en materia de información. Se resalta también el papel protagonista de las sociedades científicas en esta materia, tomando como referencia un documento sobre cribado genético en donación de gametos de la Sociedad Española de Fertilidad.

After describing the typology of the genetic tests that are developed in reproductive medicine, this paper focuses on the particularities of genetic carrier tests and genetic matching, to reason, giving examples, why the current legal framework is insufficient to respond to the controversies that arise in terms of information. The leading role of scientific societies in this area is also highlighted, taking as a reference a document on genetic screening in donation of gametes from the Spanish Fertility Society.

Palabras clave / Keywords:

Análisis genéticos / Reproducción humana asistida / Donantes de gametos / Test de portadores / *Matching* genético / Información de pruebas genéticas / Sociedades científicas.

Genetic analysis / Assisted human reproduction / Gamete donors / Carrier tests / Gene matching / Genetic testing information / Scientific societies.

1. Introducción. Tipología de los estudios genéticos en la medicina reproductiva

La medicina reproductiva es un sector en el que cada vez se genera más información genética pues los tratamientos que se llevan a cabo vienen normalmente precedidos del estudio genético de los pacientes y de los donantes de gametos, de sus gametos y embriones. En la mayoría de las ocasiones las pruebas las realizan laboratorios externos a las unidades y clínicas de fertilidad mediante técnicas de secuenciación masiva dirigida, que analizan cientos de genes y miles de mutaciones del genoma de un individuo.

Para hacerse una idea de la dimensión de esta información, tanto cuantitativa como cualitativamente, pueden tomarse dos datos muy ilustrativos: por un lado, los niños que nacen en España a través de las técnicas de reproducción asistida constituyen cerca de un 8 % de todos los nacimientos[1]; y, por otro lado, al margen de los individuos afectos de enfermedades

[1] Registro Nacional de Actividad 2016-Registro Sef (constituye actualmente el registro oficial de técnicas de reproducción asistida del Ministerio de Sanidad, Consumo y Bienestar Social). En España se han reportado en el registro de 2016, último publicado a la fecha de cierre de este trabajo, un total de 138.553 ciclos de reproducción asistida, gracias a ellas han nacido 33.472 niños lo que supone cerca de un 8 % de los nacimientos en España. Disponible en: https://www.registrosef.com/public/docs/sef2016_IAFIVm.pdf [Última consulta: 23 de julio de 2019].

monogénicas[2], todos los seres humanos son portadores de variantes patogénicas en uno o varios genes asociados a enfermedades recesivas o ligadas al cromosoma X y, cuando se emparejan para reproducirse, existe un riesgo de entre el dos y el tres por ciento de tener descendencia que padezca una enfermedad hereditaria grave[3].

Aparte de para comprobar la condición de afecto o portador de una mutación, el análisis genético puede estar dirigido de manera específica a determinar las causas de la infertilidad del paciente, centrándose en esos supuestos en el estudio de sus gametos (o de una muestra de sangre periférica). Se trataría de establecer si se producen fragmentaciones (roturas) del ADN o alteraciones cromosómicas, que den lugar a fallos de implantación o abortos de repetición.

Las pruebas pueden estar también orientadas hacia los embriones y se estaría hablando entonces de diagnóstico genético preimplantatorio, lo que en España se denominó durante muchos años DGP, pero que hoy día es conocido bajo la abreviatura PGT (test genético preimplantacional), que se subdivide, a su vez, en diversas variantes según el objetivo que persiga (PGT-A, PGT-SR y PGT-M)[4]. Además de lo anterior, estarían los casos de diagnóstico genético preimplantatorio en combinación con la determinación de antígenos de histocompatibilidad (DGP + HLA) con fines terapéuticos para terceros ("bebé salvador" de un hermano enfermo). Sobre esta técnica figuran registradas 41 solicitudes a la Comisión Nacional de Reproducción

---

[2] Está bien establecido que más de 25.000 trastornos tienen una base genética conocida (https://www.omim.org/statistics/entry), de los cuales, cerca de unos 10.000 se pueden identificar como trastornos monogénicos, esto es, la base genética está asociada a la presencia de una, o más, variantes génicas en un solo gen (http://www.who.int/genomics/public/geneticdiseases; https://www.omim.org). En contraposición, la herencia autosómica recesiva exige para que se manifieste la enfermedad que el individuo herede dos copias mutadas del mismo gen.

[3] Castilla, José Antonio / Abellán-Garcia, Fernando / Alamá, Pilar / Aura, Mónica / Bassas, Lluis / Clúa, Elisabet / De la Fuente, Luis Alfonso / Guillén, Juan José / Manau, Dolors / Rueda, Joaquín / Ruiz, Miguel / Vendrell, Xavier, *Cribado genético en donación de gametos*. Grupo de trabajo de Donación de Gametos y Embriones de la SEF, en colaboración con ASESA, AEBM-ML, ASEBIR y AEGH. Madrid: Evolhealthcare S.A.U; junio 2019. Disponible en: https://www.sefertilidad.net/docs/noticias/cribadoGenetico.pdf [Última consulta: 23 de julio de 2019]. Se apoya en los trabajos de Fujikora (2016) y Ropers (2012).

[4] PGT-A (test genético preimplantacional para aneuploidías), PGT-SR (test genético preimplantacional para anomalías estructurales), PGT-M (test genético preimplantacional para enfermedades monogénicas). Ver Brígido Llinares P. / De la Fuente Pita, R. / Del Río Riego, J. / Sanz Juste, S., "Preimplatation Genetic Testing and Biopsy Techniques", *Revista ASEBIR*, Núm. 1, Vol. 23, Julio 2018. Disponible en:
https://revista.asebir.com/assets/AF.Revista_18jul.pdf [Última consulta: 23 de julio de 2019].

Humana Asistida en los últimos cuatro años, de acuerdo con la Memoria de dicho organismo publicada en 2019[5].

Todos estos estudios (de personas afectas y portadoras, de gametos y de embriones) generan una información que constituye un caudal de datos con grandísimo potencial para aplicaciones de *big data*, tanto de uso primario (orientado a la mejora de los tratamientos de fertilidad) como secundario (dirigido a la investigación e innovación), y que permitirían profundizar no solo en el conocimiento de los factores que inciden en la infertilidad, sino también en cómo evitar numerosas enfermedades a la descendencia. La posibilidad de investigación con datos personales seudonimizados, bajo el régimen flexible que contempla la normativa de protección de datos, constituye una oportunidad para plantear proyectos a gran escala en este área del conocimiento[6].

El centro de atención de este capítulo se situará en la información obtenida a partir de los tests genéticos de portadores que se realizan a los pacientes y a los donantes, y en las controversias que se plantean desde el punto de vista ético y legal. En este sentido, se aprovecha en gran parte el trabajo "Cribado genético en donación de gametos", del Grupo de trabajo de Donación de Gametos y Embriones de la Sociedad Española de Fertilidad (SEF) (al que pertenece como único miembro jurista el autor de estas líneas), realizado en colaboración con cuatro sociedades científicas más, todas ellas referenciales en el ámbito de la reproducción humana asistida española, como son la Asociación Española de Andrología (ASESA), la Asociación Española de Biopatología Médica-Medicina de Laboratorio (AEBM-ML), la Asociación para el Estudio de la Biología de la Reproducción (ASEBIR) y la Asociación Española de Genética Humana (AEGH)[7]. Aunque se trata de entidades de ámbito estatal, para valorar la importancia del documento hay que tener presente que España es una potencia mundial en la realización de las técnicas

---

5 CNRHA. Memoria de actividades 2014-2018. Diciembre 2018. Aprobada por el Pleno el día 28 de febrero de 2019. Disponible en: http://www.cnrha.mscbs.gob.es/documentacion/comision/pdf/Memoria_Actividades_CNRHA_2014-2018.pdf [Última consulta: 23 de julio de 2019].

6 Ver definición de seudonimización en art. 4.5 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; y también la Disp. Adicional 17ª, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

7 *Cribado genético en donación de gametos*. Grupo de trabajo de Donación de Gametos y Embriones de la SEF, *op. cit.*

de reproducción humana asistida, líder europeo en número de tratamientos por delante de países mucho más poblados como Alemania o Francia[8].

Uno de los objetivos que se plantean en este trabajo es el de poner de manifiesto la insuficiencia del marco normativo para dar respuesta satisfactoria a varios de los problemas que se suscitan en este campo, particularmente de la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida (LTRA), la Ley 14/2007, de 3 de julio, de investigación biomédica (LIB) o el Real Decreto ley 9/2014, de 4 de julio, sobre calidad y seguridad en las donaciones de células y tejidos (RDLCyT).

2. Estudios genéticos con fines clínicos a pacientes y donantes de gametos

2.1. Contexto normativo de las pruebas genéticas a pacientes y donantes de gametos

En los cribados genéticos a pacientes y donantes resulta de aplicación tanto la normativa de reproducción asistida, como la de investigación biomédica. De entrada, hay que tener en cuenta que el donante de gametos es, a la postre, un paciente más a efectos de su estatus de derechos (información, consentimiento, autonomía, acceso a la documentación clínica, etc.). De esta manera, aunque la obligación genérica de informar sobre los tratamientos a pacientes y donantes se recoge en la LTRA[9], en todo lo relativo a la información y consentimiento de las pruebas concretas para conocer la condición de afecto o portador de enfermedades rigen las previsiones en materia de análisis genéticos previstas en la LIB[10]. Estos estudios consisten en obtener una muestra biológica (sangre, frotis bucal, saliva, tejido, semen, etc.) y estudiar su ADN en el laboratorio mediante una técnica de diagnóstico genético (secuenciación, PCR, MLPA[11], cariotipo, etc.), que genera una gran cantidad de

[8] V. "El coste de ser madre a los 40 alumbra una millonaria industria de reproducción asistida". *El País*, suplemento Negocios, 21 de julio de 2019. Disponible en: https://elpais.com/economia/2019/07/19/actualidad/1563549009_803035.html [Última consulta: 23 de julio de 2019].

[9] Art. 3, apartados 3 y 4, de la LTRA.

[10] V. Título V de la LIB (arts. 44 a 57).

[11] Abreviatura de Multiplex Ligation-depedent Probe Amplification, que es una técnica de biología molecular para el diagnóstico de problemas cromosómicos.

información. En algunas ocasiones puede resultar muy importante disponer de muestras biológicas de otros miembros de la familia consanguínea[12].

Cuando el estudio genético se centra en embriones humanos se está hablando de PGT (DGP), que va dirigido a seleccionar a aquellos que se encuentren libres de la alteración genética o cromosómica estudiada en cada caso. Las reglas sobre DGP son las contenidas en la LTRA, donde se prevén supuestos que pueden llevarse a cabo directamente por las clínicas y otros que requieren de una autorización de la Administración sanitaria, previo informe favorable de la Comisión Nacional de Reproducción Humana Asistida (CNRHA)[13].

2.2. Lo que dice la normativa en cuanto a las pruebas genéticas a realizar

Como se dijo anteriormente, una de las fuentes de obtención de información genética más importantes es la de los estudios de los pacientes y donantes de gametos que intervienen en la realización de las técnicas de reproducción humana asistida. Los bancos de gametos llevan a cabo pruebas genéticas a los donantes de manera sistemática conforme a los protocolos del centro, que suelen tener en cuenta, como mínimo, las recomendaciones que emanan de las sociedades científicas. También las clínicas hacen lo propio con sus donantes y pacientes. En ambos supuestos, lo normal es que se lleven a cabo estudios muy por encima de lo que exige la legalidad estricta.

En el caso de los pacientes, cuando en la consulta médica refieren antecedentes familiares de alguna enfermedad grave de posible origen genético es obligado realizar una evaluación de la carga genética para confirmar si son portadores de alguna mutación que pueda transmitir a la descendencia una enfermedad monogénica o recesiva, toda vez que el art. 3.1 de la LTRA prohíbe de forma taxativa llevar a cabo los tratamientos en los supuestos de riesgo grave para la salud, física o psíquica, de la descendencia, lo que refrenda en su articulado con la previsión de una infracción grave[14]. Si se confirma

---

[12] Ver documento informativo de estudio del paciente/donante, editado por la SEF. Disponible en: https://www.sefertilidad.net/docs/biblioteca/consentimientosESP/consentimiento28.pdf [Última consulta: 23 de julio de 2019].

[13] Art. 12 LTRA. Los únicos supuestos que no requieren informe previo de la CNRHA ni autorización son los contemplados en el apartado 1 de este precepto, esto es, los de detección de enfermedad hereditaria grave, de aparición precoz y sin tratamiento curativo posnatal en el momento presente, así como los casos de detección de otras alteraciones que puedan comprometer la viabilidad del embrión (cromosomopatías).

[14] El art. 26.2,b, 2ª, de la LTRA, describe como infracción grave la omisión de la información o los estudios previos necesarios para evitar lesionar los intereses de donantes o

una mutación patogénica de esa naturaleza, los tratamientos solo pueden llevarse a cabo si se existe posibilidad de evitarlo recurriendo a un PGT (antes DGP) de los embriones, realizando *matching* genético entre los progenitores biológicos (técnica que se explica más adelante) o bien utilizando gametos de donante para sustituir a los del progenitor portador de la mutación.

Respecto de los donantes de gametos, el art. 5.6 de la LTRA, aparte de proclamar que aquéllos deben tener más de 18 años, buen estado de salud psicofísica y plena capacidad de obrar, manifiesta que "su estado psicofísico deberá cumplir las exigencias de un protocolo obligatorio de estudio de los donantes que incluirá sus características fenotípicas y psicológicas, así como las condiciones clínicas y determinaciones analíticas necesarias para demostrar, según el estado de los conocimientos de la ciencia y de la técnica existentes en el momento de su realización, que los donantes no padecen enfermedades genéticas, hereditarias o infecciosas transmisibles a la descendencia"[15]. Esta previsión del legislador (que utiliza el verbo "demostrar") debiera haber sido quizás más prudente, pues de alguna manera induce la idea de que se puede garantizar una descendencia libre de enfermedades genéticas, lo que no es real ni siquiera realizando los tests genéticos más avanzados[16]. La realidad es que estos últimos lo más que pueden hacer es reducir la frecuencia de aparición de algunas patologías.

El citado precepto se complementa con las reglas del Anexo IV del RDLCyT, que no es sino la transposición de las directivas europeas en materia

usuarios o la transmisión de enfermedades congénitas o hereditarias. Además, el art. 18.2 de esta misma norma, proclama que los equipos biomédicos y la dirección de los centros o servicios en que trabajen incurrirán en las responsabilidades que legalmente correspondan si, entre otras cuestiones si, por omitir la información o los estudios establecidos, se lesionan los intereses de donantes o usuarios o se transmiten a los descendientes enfermedades congénitas o hereditarias, evitables con aquella información o estudios previos.

[15] Este precepto añade que estas mismas condiciones serán aplicables a las muestras de donantes procedentes de otros países; en este caso, los responsables del centro remisor correspondiente deberán acreditar el cumplimiento de todas aquellas condiciones y pruebas cuya determinación no se pueda practicar en las muestras enviadas a su recepción. En todo caso, los centros autorizados podrán rechazar la donación cuando las condiciones psicofísicas del donante no sean las adecuadas.

[16] Así lo entendió indirectamente la Sentencia 144/2016, de 30 de marzo, de la Audiencia Provincial de Valencia (Sección 7ª), al criticar esa redacción que había sido trasladada al consentimiento informado para FIV de una clínica de reproducción asistida, que resultó condenada por vulneración del derecho a la información de los pacientes: "Como acertadamente señala la sentencia de instancia, de la lectura del consentimiento informado suscrito por los demandantes, consideramos que se llega a la conclusión de que los óvulos que se van a recibir han sido sometidos a las pruebas genéticas necesarias para evitar las enfermedades que allí se indican".

de donación de células y tejidos para su uso en humanos[17], y que contempla fundamentalmente la realización de tests serológicos (HIV, Hepatitis B y C, etc.) pero no pruebas genéticas concretas. Lo más que se dice al respecto es que se llevará a cabo una evaluación de la carga genética en relación a la existencia de genes autosómicos recesivos de acuerdo al conocimiento científico y a la prevalencia conocida en la etnia del donante; y que se practicará una evaluación del riesgo de transmisión de enfermedades hereditarias conocidas y presentes en la familia. Se añade igualmente que se informará a los implicados de los resultados obtenidos de acuerdo con lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia del información y documentación clínica, y la LTRA. Esta información deberá ser lo más completa posible en relación a los riesgos asociados y a las medidas adoptadas o que se puedan adoptar, y debe ser transmitida y explicada claramente al receptor[18]. Además, en lo que no contradiga al citado RDLCyT, se tiene que tener presente igualmente el protocolo básico de donantes incluido en el Reglamento de donantes de 1996[19].

Hay que tener en cuenta que todas estas previsiones tienen más de una década, pues siendo el RDLCyT de 2014, su contenido sobre esta materia se hallaba ya literalmente presente en su antecedente normativo inmediato, que fue el Real Decreto 1301/2006, de 10 de noviembre, anulado por el Tribunal Supremo en 2014, a causa de su insuficiencia de rango normativo[20]. Han pasado más de 13 años desde entonces y eso es un mundo en el plano cien-

[17] Directiva 2004/23/CE del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativa al establecimiento de normas de calidad y de seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos; Directiva 2006/17/CE de la Comisión, de 8 de febrero de 2006, por la que se aplica la Directiva 2004/23/CE del Parlamento Europeo y del Consejo en lo relativo a determinados requisitos técnicos para la donación, la obtención y la evaluación de células y tejidos humanos; y la Directiva 2006/86/CE de la Comisión, de 24 de octubre de 2006, por la que se aplica la Directiva 2004/23/CE del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos de trazabilidad, la notificación de las reacciones y los efectos adversos graves y determinados requisitos técnicos para la codificación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos.

[18] V. letra f y g, del punto 3 del citado Anexo IV, del RDLCyT.

[19] Real Decreto 412/1996, de 1 de marzo, por el que se establecen los los protocolos obligatorios de estudio de los donantes y usuarios relacionados con las técnicas de reproducción humana asistida y regula la creación y organización del Registro Nacional de Donantes de Gametos y Preembriones con fines de reproducción humana.

[20] Sentencia de 30 de mayo de 2014, del Tribunal Supremo (Sala Tercera, Sección 4ª), dictada a raíz de un recurso contencioso-administrativo número 2/2007, promovido por la empresa Vidacord, S.L.

tífico y tecnológico, como lo ponen de manifiesto los consensos científicos que se referirán más adelante de estas líneas.

3. Un paso de gigante en la obtención de información: el análisis de portadores y el *matching* genético

3.1. ¿En qué consisten estas pruebas? Los conceptos de alto y bajo riesgo genético y de riesgo residual

El cruce de caminos entre la medicina reproductiva y la medicina genética hace ya muchos años que se vislumbraba como revolucionario, con un potencial enorme para transformar el modo de plantearse tener descendencia. El dinamismo del sector, singularmente en España, ha hecho emerger un negocio de considerables proporciones como es el de las casas comerciales y laboratorios que ofrecen los tests genéticos, que van actualizando sus paneles de enfermedades añadiendo nuevas determinaciones y consiguiendo mayor precisión diagnóstica.

El paso sustantivo en esta materia se produce cuando se confrontan los tests genéticos del varón y de la mujer (tests de portadores) que van a juntar sus gametos, para comprobar que no compartan la misma mutación recesiva, lo que podría originar que su descendencia padeciera una enfermedad. Es lo que ese conoce bajo el término de *matching* genético (emparejamiento genético), que puede utilizarse entre los miembros de una pareja heterosexual y, también, como es más frecuente hoy día, en los supuestos en que es necesaria la contribución de un donante de semen o de una donante de óvulos.

Como se dice en el citado documento sobre *Cribado genético en donación de gametos*, los estudios de portadores son estudios genéticos de cribado, dirigidos a conocer el estatus de portador o no portador de determinadas enfermedades de herencia autosómica recesiva o recesiva ligada al cromosoma X, con el objeto de establecer el riesgo genético para la descendencia de los futuros progenitores biológicos estudiados, en relación con las enfermedades incluidas en el estudio. La exactitud y precisión del emparejamiento, dependerá de la cantidad de variantes patogénicas estudiadas en cada gen.

Así, para poder determinar el riesgo reproductivo entre los dos progenitores biológicos, se emparejan los datos genéticos de uno y otro (miembro de la pareja y donante, o de dos donantes cuando la pareja o mujer sola

necesita doble donación). El *matching* se debe realizar para las enfermedades hereditarias que se trasmiten con un patrón autosómico recesivo, es decir, para aquellas en las que el problema de salud para la descendencia se origina si coinciden al mismo tiempo dos copias del mismo gen alterado (la del padre y la de la madre).

En los casos en los que no se compartan variantes en los mismos genes el *matching* se considerará de "bajo riesgo genético" y se podrá proceder a la donación de gametos habiendo reducido el riesgo de tener descendencia afectada de enfermedades hereditarias incluidas en el panel. En esta situación solo existiría el "riesgo residual"[21] de transmitir estas enfermedades debido a la limitación de la técnica (que el análisis no tenga la profundidad necesaria y pueda originarse un falso negativo). Si se comparten variantes patogénicas en los mismos genes el *matching* será de "alto riesgo genético". En este segundo caso el emparejamiento entre los gametos no se podría realizar, y el donante o la donante no deberá ser asignado a la pareja o mujer receptora[22]. Si el *matching* se ha hecho entre los miembros de una pareja, que lógicamente desean participar conjuntamente en la generación de su hijo, tendrían que contemplar otras medidas como un diagnóstico genético posterior de los embriones o recurrir a gametos de donante.

De esta forma, se lleva a cabo un estudio de compatibilidad genética entre los progenitores biológicos, que permite tomar opciones reproductivas con bastante información para evitar ciertas enfermedades en la descendencia. La potenciación de este tipo de tests genéticos abre la puerta a un futuro revolucionario desde el punto de vista de la medicina reproductiva en el que todo indica que podrán descartarse muchas patologías de base genética. No sería de extrañar que en unos años se alzaran voces que plantearan que la manera responsable de tener hijos es a través de las técnicas de reproducción asistida y el *matching* genético, y ello al margen de que la pareja sufra o no un problema de infertilidad.

---

[21] Se refiere al riesgo remanente en caso de un estudio genético con resultado negativo. Incluye aquellas variantes génicas que no ha sido posible estudiar en un determinado estudio genético y en un individuo concreto, por razones técnicas o porque se desconoce la variante responsable o por falta de conocimiento de determinadas variantes. Para estas variantes se desconoce el estatus en el sujeto estudiado. *Cribado genético en donación de gametos*, *op. cit.,* p. 10.

[22] *Cribado genético en donación de gametos*. Grupo de trabajo de Donación de Gametos y Embriones de la SEF, *op. cit.,* pp. 23-24.

3.2. Problemas de información en torno a los tests de portadores y el matching genético

3.2.1. El alcance de la información: el criterio de la LIB y sus limitaciones aplicadas a las pruebas genéticas de la medicina reproductiva

Se ha dicho más arriba de estas líneas que en lo referente al consentimiento informado sobre las pruebas genéticas deben regir las previsiones de la LIB (ya que la LRHA no aborda más pruebas genéticas que las embrionarias), pero, como se comentará a continuación, esta norma no responde satisfactoriamente al campo de la medicina reproductiva, en particular al tratar de la realización de tests genéticos de portadores y del *matching* genético.

La primera cuestión a resaltar es la del envejecimiento natural de la LIB derivado del cambio del contexto científico desde que se promulgó, hace más de doce años, hasta el momento actual. Cuando entró en vigor la ley los análisis genéticos se llevaban a cabo para detectar mutaciones concretas, que eran las que justificaban su realización por existir una sospecha de acuerdo con los antecedentes clínicos del paciente. Sin embargo, la generalización (por su abaratamiento) de las pruebas de secuenciación masiva (NGS)[23] a partir de la primera década del siglo XXI, supusieron un cambio fundamental en el estudio genético por el aumento exponencial de la cantidad de información obtenida de cada análisis, lo que condujo, a su vez, a un incremento extraordinario de la complejidad a la hora de valorar las implicaciones y trascendencia de estas pruebas.

Es cierto que la LIB expone que el contenido de la información que se debe transmitir al paciente ha de abarcar la explicación sobre las consecuencias para el afectado y su descendencia del diagnóstico genético resultante y las posibles alternativas[24], y, además, que prevé que se advierta al paciente sobre la posibilidad de descubrimientos inesperados y su posible trascendencia para el sujeto, así como sobre la facultad de éste de tomar una posición respecto a recibir o no su comunicación[25], pero estas proclamaciones parten de la idea de que la "toma de posición" del paciente se proyecta

[23] Secuenciación masiva (NGS): del inglés "Next Generation Sequencing", se refiere a una técnica de análisis genético de alto rendimiento, que se utiliza para determinar la secuencia de nucleótidos de la totalidad, o una porción, del genoma de un individuo. V. *Cribado genético en donación de gametos*, *op. cit.,* p. 61.

[24] Arts. 3 e) y 55.2 de la LIB.

[25] Art. 47.4º de la LIB, en relación con lo establecido en el art. 4.5 del mismo texto legal, donde se dice que "toda persona tiene derecho a ser informada de sus datos genéticos y

sobre un escenario más o menos acotado, que es capaz de comprender y en el que su decisión puede adoptarse con verdadero conocimiento de causa, es decir, siendo consciente de las implicaciones de su postura. Sin embargo, con la secuenciación masiva, con la aplicación de los tests de portadores en combinación con la práctica del *matching* genético asociado a las técnicas de fertilidad, razonablemente un paciente medio estará desbordado por la complejidad de la información que se va a obtener, esto es, no se hallará en condiciones de pronunciarse. A modo de ejemplo, en los resultados de un análisis genético existen variantes de significado incierto (conocidas como VUS o VOUS)[26], pero que pueden dejar de serlo a lo largo del tiempo o respecto de las que puede haber distintas interpretaciones.

Por razón de la citada complejidad, de la asimetría tan acusada en materia de información entre los profesionales y los pacientes (y donantes), tal y como se explicará en el punto siguiente, la recomendación que se hace en el Documento de cribado genético a los pacientes es la de que deleguen en el equipo médico la conveniencia de comunicar o no los hallazgos inesperados[27]. Otras sociedades científicas, como el Colegio Americano de Genética y Genómica, optan por establecer listados de hallazgos patogénicos o probablemente patogénicos, que van actualizando, y que consideran deberían ser informados en todo caso a los pacientes[28].

Sucede además que en los tratamientos de fertilidad en los que intervienen donantes, la información genética que puede interesar a un paciente no es solo la suya propia, sino la del donante en cuanto progenitor biológico de su hijo, lo que plantea el problema de hasta qué punto la pareja o mujer

---

otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad".

[26] El acrónimo VUS o VOUS responde a "variant of unknown significance". Se trata de una variante de la que se tienen evidencias limitadas, o interpretaciones contradictorias, respecto a su efecto patogénico. Su efecto biológico es incierto y no es posible basar las decisiones clínicas en función de estas variantes. Actualmente, la mayoría de sociedades científicas recomiendan que los paneles de cribado genético ampliados de portadores sólo informen de las variantes que afecten claramente a la función del gen y que las VUS no sean reportadas (Edwards et al., 2015). V. *Cribado genético en donación de gametos*, *op. cit.* p. 12.

[27] Se trata de una opción que figura en el mencionado documento informativo de estudio del paciente/donante, editado por la SEF. Disponible en: https://www.sefertilidad.net/docs/biblioteca/consentimientosESP/consentimiento28.pdf [Última consulta: 23 de julio de 2019].

[28] *Cribado genético en donación de gametos*. *ob. cit.* p. 28. Se refiere a *The American College of Medical Genetics and Genomics* (ACMG) y sus recomendaciones publicadas en 2014 (Green *et ál.*, 2013) y actualizadas en 2016 (Kalia, 2017).

sola receptora puede conocer esos estudios de una tercera persona. La LIB no contempla este supuesto concreto[29], mientras que la LRHA se limita a reconocer el derecho de los hijos y de la receptora, por sí o por sus representantes legales, a obtener información general de los donantes que no incluya su identidad; y a decir que los datos de las historias clínicas, excepto la identidad de los donantes, deberán ser puestos a disposición de la receptora y de su pareja, o del hijo nacido por estas técnicas o de sus representantes legales cuando llegue a su mayoría de edad, si así lo solicitan[30]. En el caso de la LRHA (2006), como se ha dicho pasa también con la LIB (2007), el legislador difícilmente podía imaginarse la relevancia de la secuenciación masiva ni el desarrollo espectacular de los tests genéticos, y por eso las citadas previsiones no abordan realmente la problemática mencionada.

En las técnicas de fertilidad debe tenerse en cuenta, como factor limitador de la información, que rige la regla del anonimato del donante[31], lo que, añadido a su derecho a la intimidad y a la protección de sus datos personales, constituyen una barrera importante para el acceso libre al resultado del estudio genético de aquél a instancia de una pareja receptora. Esto conduce a la necesidad de llevar a cabo una valoración ponderada de cada caso de solicitud de información que se presente para comprobar cuáles son las necesidades reales de conocer la información genética del donante, lo que normalmente estará en función del problema de salud (del hijo) que se tenga delante. Bien es cierto que en el plano teórico podría haber supuestos excepcionales de peligro cierto para la vida o la salud del hijo en los que estuviera justificada incluso la revelación de la identidad del donante, como de hecho

[29] Es cierto que en el art. 4.5 in fine, de la LIB establece que "se respetará el derecho de la persona a decidir que no se le comuniquen los datos a los que se refiere el apartado anterior, incluidos los descubrimientos inesperados que se pudieran producir. No obstante, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades"; ahora bien, los donantes de gametos no son familiares de las parejas receptoras y, por tanto, esta previsión no se refiere a ellos.

[30] Arts. 5.5 y 18.3 de la LRHA. La facultad de información referida en los dos preceptos anteriores debe entenderse ejercitable en un momento posterior al transfer de los gametos o embriones, ya que si fuera antes permitiría a los pacientes seleccionar las características del donante, lo que está vedado en la ley. En consecuencia, aquella información de trascendencia clínica que, en su caso, pidieran los pacientes, siempre que estuviera justificada y no comprometiera la identidad del donante (esta es la línea roja), debería facilitárseles, especialmente en los supuestos en que naciera un niño con un problema grave de salud.

[31] Art. 5.5 de la LRHA.

contempla la LRHA[32]. En todo caso, el principio de proporcionalidad debe aplicarse siempre en estas situaciones para tratar de salvaguardar la mayor parte de los derechos y valores en juego, y los grandes protagonistas en esa ponderación han de ser los equipos médicos de los centros, pues la LRHA no obliga a judicializar estos conflictos.

3.2.2. Reanálisis y nuevos hallazgos ¿Cuándo es obligado recontactar?

La participación de donantes origina una problemática más controvertida todavía, como es la de que puedan conocerse nuevos hallazgos con trascendencia para su salud y para la de sus descendientes biológicos. Como punto de partida, debe admitirse que ni los bancos de gametos ni las clínicas y unidades hospitalarias de fertilidad tienen obligación de llevar a cabo reanálisis de las muestras biológicas de donantes y pacientes, ni reinterpretaciones de los estudios ya efectuados, conforme avanza el estado de la ciencia. Lógicamente, los equipos médicos han de aplicar los protocolos y recomendaciones médicas de estudio de los pacientes y donantes que estén vigentes en el momento en que se llevan a cabo las técnicas, esto es, la *lex artis* médica de ese tiempo, y no se les puede pedir que reinterpreten los resultados periódicamente a la luz de nuevos descubrimientos sobre el genoma, ya que eso conduciría a una exigencia desproporcionada, ilimitada en el tiempo e imposible de atender en todos los órdenes (asistencial, logístico, económico, jurídico, etc.). Por otro lado, si se impusiera una obligación de esa naturaleza no habría compañía de seguros que cubriera la responsabilidad profesional de los equipos médicos, ante la eventualidad de pacientes que reclamaran a las clínicas por no haberles advertido de nuevas interpretaciones de la información genética que se obtuvo años atrás del donante (progenitor biológico de sus hijos) o de ellos mismos.

Muchas clínicas de fertilidad, conscientes del problema legal que podría originárseles, únicamente reciben del laboratorio de genética (normalmente un centro externo) un informe que se limita a confirmar la compatibilidad o no del donante con la parte receptora (del *matching* genético), de forma que no disponen, por voluntad propia, de los resultados completos de las pruebas y así lo advierten a los pacientes.

[32] Art. 5.5 in fine, de la LRHA, que dice: "Sólo excepcionalmente, en circunstancias extraordinarias que comporten un peligro cierto para la vida o la salud del hijo o cuando proceda con arreglo a las Leyes procesales penales, podrá revelarse la identidad de los donantes, siempre que dicha revelación sea indispensable para evitar el peligro o para conseguir el fin legal propuesto. Dicha revelación tendrá carácter restringido y no implicará en ningún caso publicidad de la identidad de los donantes".

Entonces, ¿por qué se producen nuevos hallazgos en relación a los donantes de gametos?. Las situaciones más frecuentes son dos: la primera, porque se descubre que un niño nacido a raíz de las técnicas con participación de un donante de gametos presenta una enfermedad genética, hereditaria y grave que no estaba incluida en los paneles que se utilizaron en su momento. Conocido un supuesto de esta naturaleza, resulta obligado bloquear los gametos que puedan quedar de ese donante (para que no se utilicen en otras receptoras en lo que se aclara la situación), dar la alerta correspondiente (por si pudiera haber más casos) y plantearse recontactar con él (o ella) y con el resto de descendientes a que puedan haber dado lugar (otras familias que utilizaron gametos del mismo donante), para ofrecerles estudiar el caso realizando nuevas pruebas, todo ello bajo las reglas de la LIB (consentimiento informado, indicación médica, asesoramiento genético, etc.).

La segunda situación típica en la que pueden conocerse hallazgos inesperados por un reanális, sería la de un donante que repite años después de la primera donación, y al que en la segunda ocasión se le aplican unos protocolos más avanzados que incluyen el diagnóstico de un número de enfermedades superior a las que se chequearon inicialmente. Si se constata que el donante tiene una mutación que en potencia puede ser causante de una enfermedad grave, surge también la controversia de si recontactar o no con las familias que tuvieron hijos de ese donante.

Sobre esta cuestión, en el documento de *Cribado genético en donación de gametos* se incluye la siguiente conclusión: "el manejo de la información genética, tanto en donantes como en las parejas que se benefician de los programas de donación, debe realizarse en el contexto de un adecuado asesoramiento genético previo y posterior a los estudios genéticos que se indiquen en cada caso. Respecto a la posibilidad de recontactar con los pacientes y donantes por nuevos hallazgos, se considera que el criterio para decidir si hacerlo o no debería de fijarse en aquellas situaciones concretas con trascendencia clínica significativa para la receptora, su descendencia o para los propios donantes (pensando en su proyecto reproductivo futuro), a juicio del equipo médico. Es decir, que sí procedería recontactar en aquellos supuestos en los que la patología se considere, desde el punto de vista médico, relevante para la salud del afectado y, razonablemente, sea posible tomar alguna medida preventiva o curativa. Se recomienda aconsejar a los pacientes y donantes que deleguen la decisión de cuándo recontactarles en el equipo médico"[33].

[33] *Cribado genético en donación de gametos*. *op. cit.* pp. 49-50.

En consecuencia, el criterio de la trascendencia clínica para el afectado se antoja como clave en materia de información sobre hallazgos inesperados, tanto a la hora de comunicar el resultado de los análisis propios, como para decidir si recontactar para advertir de un descubrimiento en relación a los donantes de gametos. Esta solución coincide con la apuntada por los profesores Romeo Casabona, Nicolás Jiménez y De Miguel Beriain, cuando emplean el concepto de "utilidad clínica" como criterio clave que activa la obligación de información, incluyendo entre esa información a transmitir la que pueda ser relevante para la toma de decisiones reproductivas[34].

Más discutible es si en este terreno, el que está en juego la salud de la descendencia, puede admitirse el ejercicio del derecho a no saber de los progenitores. Como se dice igualmente en el documento de *Cribado genético en donación de gametos*, se pueden distinguir dos situaciones distintas: "por un lado, la renuncia a la información del estudio personal y, por otro lado, la renuncia a la información del estudio del donante, singularmente cuando se ha ampliado el estudio de este último con ocasión de otras donaciones posteriores. Pues bien, respecto de este segundo supuesto, cuando la información del donante pueda tener importancia para la salud de la descendencia (y se trate de menores de edad), resulta difícil admitir desde el punto de vista ético que sus padres o representantes puedan rechazarla, ya que el menor quedaría desprotegido (su mayor interés pasaría sin duda por el hecho de que se tuviera en cuenta esa información). Por este motivo, se considera que no se debe aceptar la renuncia a la información del donante cuando, a juicio del equipo médico, tenga trascendencia clínica significativa para un descendiente menor de edad"[35].

---

[34] Romeo Casabona, Carlos María / Nicolás Jiménez, Pilar / De Miguel Beriain, Íñigo, *Retos éticos y necesidades normativas en la actividad asistencial. En medicina personalizada de precisión*. Fundación Instituto Roche, 2018. V. apartado 4.1.2, pp. 48-50. Los autores manifiestan: "En cuanto a la utilidad clínica, significa que el análisis representa un beneficio para el manejo clínico del enfermo o sus familiares (diagnóstico, tratamiento o seguimiento) o evita la realización de otros procedimientos diagnósticos o terapéuticos inapropiados o proporciona información clave para la toma de decisiones reproductivas del individuo o de sus familiares que pueden comprometer a su descendencia. Pues bien, si un análisis genético se puede realizar con estos fines, para los que se reconoce su utilidad, lo mismo puede decirse de la obligación de información de sus resultados. Es decir, la información que debe ser transmitida abarca toda aquella que incida en un proceso clínico pero también la que pueda ser relevante para la toma de decisiones reproductivas, tanto si su detección motivó el análisis, como si se tratara de un hallazgo secundario o inesperado". Disponible en: https://www.institutoroche.es/static/pdfs/Retos_eticos_necesidades_normativas_MPP.pdf [Última consulta: 23 de julio de 2019].

[35] *Cribado genético en donación de gametos*, *op. cit.,* p. 41.

El derecho a no saber se proyecta sin duda, y con especial intensidad, cuando se trata de la realización de análisis genéticos, ya que los pacientes pueden querer legítimamente protegerse del impacto en su vida de informaciones que puedan crearles preocupación, angustia o, incluso, desesperación[36]. Sin embargo, cuando esa renuncia afecta a terceros, como son sus hijos (ya nacidos), la virtualidad de ese derecho es cuestionable desde el punto de vista ético. En el plano legal, podría invocarse la aplicación de la previsión de la LIB para los casos de grave perjuicio para la salud de un familiar biológico, que contempla que se pueda comunicar a un familiar próximo[37], aunque no esté pensada expresamente para el campo de los tratamientos de fertilidad, ya que por lógica son los padres o representantes legales del menor a los que concierne de manera directa esta cuestión, y no a los familiares de aquéllos.

Todas estas consideraciones sugieren la conveniencia de reformar la LRHA, para incluir una regulación de las pruebas genéticas aplicadas a los tratamientos de fertilidad, lo que debería hacerse con la extensión suficiente para crear un marco amplio de actuación.

3.2.3. La importancia de la Sentencia de la Audiencia Provincial de Valencia de 2016. Obligada información sobre la limitación de los estudios genéticos

En el terreno de la información genética relacionada con las técnicas de reproducción humana asistida ha tenido gran importancia el pronunciamiento de la Audiencia Provincial de Valencia de 2016, por el que se condenó a una clínica de fertilidad a satisfacer una indemnización de 400.000 €[38]. No en vano esta resolución propició un reajuste de los consentimientos informados de la SEF para incluir expresamente lo relacionado con las pruebas genéticas.

---

36 Abellán, Fernando: "El derecho a no saber la información genética. El caso del País Vasco de reconocimiento a favor de una pareja con antecedentes familiares de Corea de Huntington", *Revista Derecho y Genoma Humano / Law and the Human Genome Review,* Núm. 43, 2015, pp. 163-171.

37 Art. 4.5 *in fine*, de la LIB, ya mencionado, que establece que "…, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades"

38 Sentencia núm. 144/2016, de 30 de marzo, de la Audiencia Provincial de Valencia (Sección 7ª). La condena de 400.000 € se desglosó en 100.000 € a cada uno de los padres y otros 200.000 € al menor.

El supuesto enjuiciado trataba de una pareja que había acudido a una clínica de fertilidad para tener un hijo, teniendo que recurrir a óvulos procedentes de donante. Tres meses después de confirmarse el embarazo la pareja recibió una llamada del médico para informarles de que, de la misma donante de óvulos, había nacido en Alemania un niño con una hemofilia severa tipo A, y proponerles hacerse unas pruebas para constatar si el feto podría estar afecto y, en su caso, valorar una interrupción voluntaria del embarazo. A pesar de comprobarse el resultado positivo de la prueba, por lo avanzado de la gestación y por sus convicciones morales, la pareja decidió seguir adelante y tener su hijo, que nació con hemofilia.

Tras ello, formularon una reclamación a la clínica al considerar que en esta última no se habían hecho los controles adecuados de la donante para descartar la transmisión de la patología. La Audiencia Provincial valoró dos aspectos distintos: por un lado, si la actuación había sido correcta desde el punto de vista técnico, concluyendo que razonablemente el test de la hemofilia no estaba indicado llevarlo a cabo de manera sistemática y que en el caso clínico la paciente no había referido ningún antecedente familiar de la enfermedad (aparentemente se trataba de una mutación surgida *ex novo*). En consecuencia, para el tribunal el resultado no podía ser imputado al equipo médico de la clínica por culpa o negligencia.

Y, por otro lado, estudió la cuestión de la información a los pacientes sobre las pruebas genéticas, haciendo los siguientes reproches al modelo de consentimiento informado que se había utilizado: no se comunica la realidad sobre las pruebas y análisis a los que se han sometido a los gametos, no se advierte de que no se hacen pruebas genéticas de muchas enfermedades detectables, no se advierte tampoco de que hay muchas enfermedades genéticas que no pueden detectarse todavía, y no se informa "con claridad y precisión" de que siempre va a existir un riesgo de transmisión de enfermedades. A la postre, la Audiencia Provincial cuestionó la falsa sensación de seguridad que se transmitía a los pacientes al mencionar en el consentimiento informado las pruebas genéticas incluidas en el protocolo del centro, y consideró que se había vulnerado el derecho de información de los pacientes, incurriendo por ello la clínica en la correspondiente responsabilidad civil.

Como se dijo más arriba, esta Sentencia condujo a una modificación de los consentimientos de la SEF, que dio lugar a que se introdujera, por ejemplo, respecto de la técnica de Fecundación in vitro (FIV), un apartado específico de "riesgos genéticos", donde se dice que "no puede descartarse completamente la presencia de enfermedades genéticas en la descendencia.

Los estudios genéticos permiten solamente disminuir la frecuencia de su aparición en algunos casos". Y, también, en el apartado informativo para el caso de utilización de gametos o embriones procedentes de donante, una mención al carácter limitado de las pruebas genéticas, así como la prevención de que "hay muchas mutaciones o alteraciones de origen genético que no pueden detectarse, por lo que no cabe descartar completamente el riesgo de transmisión de una enfermedad genética a la descendencia"[39]. En definitiva, esta resolución judicial supuso un punto de inflexión para los profesionales de la reproducción asistida en materia de información sobre las pruebas genéticas, que ha propiciado una mayor mesura y contención a la hora de explicar a los pacientes las ventajas de los tests genéticos, desterrando la idea errónea de que se puede garantizar un hijo sano.

3.2.4. El papel de las sociedades científicas para fijar criterios de normopraxis. La aceptación o rechazo de los donantes en función de su información genética

En un campo de tanto dinamismo como el de la medicina genética reproductiva, donde las novedades se suceden constantemente, no es fácil que el legislador tenga actualizado el estado de la ciencia en relación a las pruebas a realizar a pacientes y donantes. Ya se dijo más arriba que en el caso de tratamientos con donantes de gametos se realizan de rutina análisis genéticos para tratar de evitar que se transmitan enfermedades hereditarias, y el alcance de esas pruebas va ampliándose conforme se tienen más datos de estudios publicados y en la medida en que también avanza la tecnología.

En este escenario cobra una importancia capital el papel de las sociedades científicas, como entidades donde se deben generar los consensos profesionales en materia de recomendaciones, guías clínicas y protocolos. La autoridad de los documentos de consenso de las sociedades científicas no cabe duda que está en relación directa con su prestigio y reputación, ya que no hay una mención específica en la normativa que las refrende en este terreno. A las sociedades científicas se las cita como colaboradoras y asesoras de la Administración pública fundamentalmente respecto de la formación continuada tanto en la Ley de ordenación de las profesiones sanitarias[40]

[39] V. Documento informativo de Fecundación in vitro o microinyección espermática (FIV/ICSI) y criopreservación de preembriones, de la SEF. Disponible en: https://www.sefertilidad.net/docs/biblioteca/consentimientosESP/consentimiento3.pdf [Última consulta: 23 de julio de 2019].

[40] Arts. 28.1, c, 34 y 38 de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

como en la Ley de cohesión de calidad del Sistema Nacional de Salud[41]. Indirectamente se reconoce su importancia en la primera de las leyes citadas cuando, a la hora de definir los principios generales de actuación de los profesionales sanitarios, se establece que estos últimos tendrán como guía de su actuación el servicio a la sociedad, el interés y salud del ciudadano a quien se le presta el servicio, el cumplimiento riguroso de las obligaciones deontológicas, determinadas por las propias profesiones conforme a la legislación vigente, y de los criterios de normo-praxis o, en su caso, los usos generales propios de su profesión[42]. Estos criterios de normo-praxis, e incluso en algunos casos los usos de la profesión, son definidos precisamente por las sociedades científicas a través de documentos de recomendaciones y protocolos de actuación que, como la misma norma indica, deberán ser utilizados de forma orientativa, como guía de decisión para todos los profesionales de un equipo, y serán regularmente actualizados con la participación de aquellos que los deben aplicar[43]. La sede donde los profesionales pueden actualizar mejor sus recomendaciones y protocolos (dejando al margen los de uso interno de los centros) es su sociedad científica donde, en el seno de sus grupos de trabajo y en las reuniones y congresos, cambian impresiones, contrastan y aplican sus conocimientos, experiencia y publicaciones. En el campo de fertilidad, es un hecho que la labor de las sociedades científicas viene siendo crucial para recomendar qué pruebas procede realizar a los donantes de gametos y proponer criterios de actuación en distintas situaciones, de acuerdo con el estado de la ciencia.

Debido a que todas las personas son portadores de variantes patogénicas, y eso incluye lógicamente a los donantes de gametos, cabe preguntarse en qué circunstancias de salud genética debe rechazarse a un donante. Parece claro que habría que descartarle respecto de un paciente (hombre o mujer) con el que compartiera variantes patogénicas en el mismo gen, puesto que con gran probabilidad nacería un niño afecto de la enfermedad. Para eso precisamente se aplica el *matching* genético, para hacer el emparejamiento y comprobar la compatibilidad o no entre dos progenitores biológicos. Sin embargo, si las mutaciones del donante (de semen u ovocitos) y paciente son distintas no habría problema en utilizar a ese donante, a pesar de que fuera portador de las mutaciones, ya que el descendiente no padecería la enfermedad. Es decir, los gametos de determinado donante podrían ser

[41] Arts. 34 a, 35.2 c, 53.1 d, 60.2, 64.1 y 67.3 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
[42] Art. 4.5 de la Ley 44/2003.
[43] Art. 4.7, b, de la misma Ley 44/2003.

válidos para un paciente y no para otro distinto (siempre que se trate de enfermedades con patrón de herencia autosómico recesivo).

Los bancos de gametos aplican sistemáticamente a los donantes los test ampliados de portadores para conocer de qué enfermedades son portadores y tenerlos listos para hacer un *matching,* mientras que los pacientes no siempre aceptan realizarse ese tipo de pruebas (por el coste, por decisión íntima personal, etc.). Se plantea entonces si se pueden utilizar gametos de donantes que tienen hecho el test de portadores en parejas que no han querido hacerse esa prueba ni el subsiguiente *matching* genético, y es aquí donde el documento de *Cribado genético en donación de gametos* incorpora unas pautas a tener en cuenta:

En primer lugar, fijando el cribado genético básico para los donantes que incluye una serie de variantes que, por su prevalencia, penetrancia y gravedad, deben analizarse obligatoriamente[44]. En segundo lugar, estableciendo que los gametos de donantes que presenten variantes patogénicas para las enfermedades incluidas en el cribado genético básico, solo podrán ser utilizados cuando se descarte la existencia de variantes patogénicas en el receptor a través del *matching* genético. Y, en tercer lugar, proclamando que un donante portador de enfermedades recesivas de baja prevalencia, entendiendo por tales las patologías con una frecuencia de portadores más baja de 1/60, puede ser utilizado sin que se conozca el estatus genético en el receptor, y ello sin perjuicio de que los pacientes deban ser informados de esta circunstancia en el consentimiento informado[45]. En definitiva, por debajo del citado indicador se considera que el riesgo de recurrencia en la futura descendencia es bajo.

Evidentemente estos criterios no son de naturaleza legal, y por ello no vincularían obligatoriamente a los tribunales que eventualmente conocieran

---

[44] *Cribado genético en donación de gametos*, *op. cit.,* p. 48. El cribado básico incluye el análisis de variantes patogénicas relacionadas con la fibrosis quística (CFTR), la atrofia muscular espinal (SMN1), sordera neurosensorial no sindrómica (GJB2) y hemoglobinopatías más prevalentes (HBA1/HBA2, HBB; alfa y beta talasemia, anemia falciforme). Y en donantes de ovocitos, además, estudio molecular del gen FMR1 relacionado con el Síndrome del X frágil.

[45] *Cribado genético en donación de gametos*, *op. cit*., p. 49. Se añade que en el caso del estudio molecular del Síndrome del X-Frágil, serán descartados según el riesgo de transmitir dicho síndrome, y que, en cualquier caso, se descartarán donantes de ovocitos con variantes patogénicas en genes de herencia ligada al cromosoma X. Estos descartes exigirían que se informara confidencialmente a la donante de las razones, de acuerdo con lo previsto en el art. 6.3 del Real Decreto 412/1996, de 1 de marzo.

de una posible reclamación por el nacimiento de un niño con una enfermedad genética, pero no cabe duda de que tienen indudable fuerza de autoridad como referencia prudente y expresión del consenso científico, plasmado en un documento avalado por las sociedades científicas españolas más importantes en el campo de la fertilidad. Por este motivo, estas reglas así surgidas se transforman en un elemento de normo-praxis (que debe respetarse con carácter orientativo de acuerdo con la citada Ley de ordenación de las profesiones sanitarias) y que integra la *lex artis* médica de este campo profesional, en tanto no sean modificadas por un nuevo consenso científico que pudiera generarse.

3.2.5. Otros aspectos controvertidos en relación a estas pruebas

Al contrario de lo que sucede con otro tipo de avances médicos (por ejemplo, en el terreno de los medicamentos), las novedades relacionadas con los tests genéticos se difunden y comercializan sin que haya dado tiempo a hacer ensayos y estudios prospectivos que midan su eficacia y seguridad, su incidencia real en la mejoría de salud de los recién nacidos. Aparentemente una pareja que utiliza un test que incluya 500 enfermedades tendrá más oportunidades de tener descendencia libre de enfermedades que otra que utilice uno cuyo panel solo tenga 250 o que simplemente no utilice ningún test, pero eso por sí solo no prueba (al menos no como dicta la metodología científica) que las parejas que los utilizan tengan realmente hijos más sanos que las que no lo hacen (o que la diferencia sea significativa en términos globales). Sin embargo, la publicidad de los laboratorios de genética, de las casas comerciales de estos tests e incluso de algunas clínicas de fertilidad, se apoya de manera muy notable en la existencia de estas pruebas –de la cantidad de enfermedades que teóricamente pueden evitarse– como reclamo de sus servicios. Esta situación obliga a realizar una reflexión crítica sobre el verdadero alcance de estos estudios, sobre la honestidad de la información que se traslada a los pacientes, y aquí una vez más es muy importante la labor de las sociedades científicas para poner en su justa medida sus ventajas y evitar crear falsas expectativas (como la de garantizar un niño libre de enfermedades).

Al margen de lo anterior, la proliferación de las pruebas genéticas en el campo de los tratamientos de fertilidad, conduce a que los clásicos problemas tantas veces comentados en este terreno de posible lesión a la intimidad (si no se salvaguarda la seguridad de las bases de datos generadas) y de desigualdad social (si no se asegura un acceso equitativo para las familias

con menos recursos), lejos de mitigarse se potencien de manera notable. El llamamiento que se hace en el documento de *Cribado genético en donación de gametos*, respecto de la posibilidad de desigualdades no deja lugar a la duda al afirmar: "las desigualdades sociales no son desde luego algo nuevo en la sociedad, pues siempre las familias con más medios económicos han podido sufragar una mejor educación y oportunidades para sus hijos que el resto de familias. Sin embargo, las desigualdades que se plantean en este terreno guardan relación con un factor distinto y singular, como es el hecho biológico de concebir con mayor probabilidad hijos sanos, lo que supone un factor de desigualdad en el plano ontológico y, por tanto, de más calado y profundidad. Los poderes públicos tienen que provocar el debate social sobre estas cuestiones y tratar de fijar consensos que garanticen la accesibilidad a aquellas prestaciones que demuestren una clara mejora de la salud"[46].

La desigualdad en el acceso a los tests genéticos de portadores y al *matching* genético es una realidad hoy día por cuanto estas pruebas solo se ofrecen en las clínicas privadas. Constituye por tanto un reto a futuro que el Sistema Público de Salud pueda ir incorporando algunas de estas pruebas dentro del catálogo de prestaciones para que sus ventajas alcancen a toda la población que las necesite.

4. Conclusiones

Las pruebas genéticas que se llevan a cabo en la medicina reproductiva responden a una casuística específica y por ello presentan también unas particularidades propias en el terreno ético y jurídico.

La secuenciación masiva y los tests de portadores en combinación con el *matching* genético, realizadas en el contexto de las técnicas de reproducción humana asistida, generan una gran cantidad de información que, debidamente sistematizada, permitiría desarrollar proyectos de *big data* con un potencial enorme para la mejora de los tratamientos y para la eliminación de muchas enfermedades en la descendencia.

Las citadas pruebas genéticas originan controversias en materia de información que desbordan el marco actual de la Ley de investigación biomédica

[46] *Cribado genético en donación de gametos*, *op. cit*, p. 42. Ver también Abellán, Fernando, "Bioética y Sociedad: la participación de los ciudadanos en el debate bioético", *Investigación en Bioética*, Feito, Lydia / Domingo, Tomás (Coords.), Univ. Rey Juan Carlos y Dykinson, 2012, pp. 315-334.

y de la Ley de reproducción asistida. En este sentido, sería deseable una modificación de esta última para incluir un capítulo específico que recogiera estos estudios.

Debido al dinamismo de medicina genética reproductiva, las sociedades científicas de este campo, como colaboradoras de la Administración sanitaria, son las entidades más adecuadas para actualizar el conocimiento médico y científico y para fijar los criterios de normo praxis que deban regir en cada momento.

5. Bibliografía

Abellán, Fernando, "El derecho a no saber la información genética. El caso del País Vasco de reconocimiento a favor de una pareja con antecedentes familiares de Corea de Huntington", *Revista Derecho y Genoma Humano / Law and the Human Genome Review,* Núm. 43, 2015.

Abellán, Fernando: "Secuenciación genómica masiva e información. Nuevos retos", *Informe del Experto*, Núm. 10, Fundación Merck Salud, Octubre 2014.

Brígido Llinares, Paula / De la Fuente Pita, Roberto / Del Río Riego, Javier / Sanz Juste, Sara, "Preimplatation Genetic Testing and Biopsy Techniques", *Revista ASEBIR*, Núm. 1, Vol. 23, 2018.

Castilla, José Antonio / Abellán-Garcia, Fernando / Alamá, Pilar / Aura, Mónica / Bassas, Lluis / Clúa, Elisabet / De La Fuente, Luis Alfonso / Guillén, Juan José / Manau, Dolors / Rueda, Joaquín / Ruiz, Miguel / Vendrell, Xavier, *Cribado genético en donación de gametos*. Grupo de trabajo de Donación de Gametos y Embriones de la SEF, en colaboración con ASESA, AEBM-ML, ASEBIR y AEGH, Evolhealthcare S.A.U, Madrid, España, junio 2019.

Cnrha. *Memoria de actividades 2014-2018*. Diciembre 2018. Aprobada por el Pleno el día 28 de febrero de 2019.

Romeo Casabona, Carlos María / Nicolás Jiménez, Pilar / De Miguel Beriain, Íñigo, *Retos éticos y necesidades normativas en la actividad asistencial. En medicina personalizada de precisión*, Fundación Instituto Roche, 2018.

Sánchez-Caro, Javier / Abellán, Fernando (Coords.), *Medicina genética clínica del siglo XXI. Consideraciones científicas, éticas y legales*, Fundación Salud 2000 / Ed. Comares, Granada, España, 2009.

Sánchez-Caro, Javier / Abellán, Fernando, *Bioética y ley en reproducción humana asistida. Manual de casos clínicos*, Fundación Salud 2000 / Ed. Comares, Granada, España, 2009.

Evaluación de proyectos de investigación con tecnología *Big Data* por un Comité de Ética de la investigación*

Evaluation of research projects with Big Data technology by a Research Ethics Committee

Iciar Alfonso Farnós

Comité de Ética de la Investigación con medicamentos de Euskadi (Vitoria, España)

Guillermo Alcalde Bezhold

Comité de Ética de la Investigación Hospital Universitario Araba (Vitoria, España)

Miriam Méndez García

Comité de Ética de la Investigación con medicamentos Hospital Clinic Barcelona (Barcelona, España)

DOI: 10.14679/1141

Sumario / Summary: 1. Introducción. 2. Control ético. 2.1. Principios éticos. 2.2. Recomendaciones internacionales. 3. Marco normativo. 3.1. Ley 14/2007, de 3

* Artículo recibido el 21 de marzo de 2019 y aceptado para su publicación el 16 de junio de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos –*Big Data*–. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER).

de julio, de Investigación biomédica. 3.2. La Ley de Autonomía del Paciente. 3.3. Reglamento Europeo de protección de datos. 3.4. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. 4. Aspectos adicionales que deben revisar los CEI, en la evaluación de proyectos de investigación, en cumplimiento de las exigencias del nuevo marco normativo en materia de protección de datos. 5. Criterios que debe aplicar un CEI en la evaluación de proyectos de investigación con tecnología *big data*. 6. Adaptación de los CEI a la evaluación de proyectos con tecnología *big data*. 7. Seguimiento de la investigación de estudios big data por los comités. 8. Conclusiones.

Resumen / Abstract: La investigación con tecnología *Big Data* en el ámbito sanitario debe realizarse en el contexto de un marco ético y jurídico que garantice el máximo nivel de protección en el tratamiento de datos de carácter personal. Los comités de ética de la investigación, como garantes de los derechos, seguridad y bienestar de los sujetos que participan en un proyecto de investigación biomédica, deben verificar el cumplimiento de los principios éticos y legales aplicables a la investigacion con datos de salud. En este trabajo se revisan los principios éticos y legales aplicables a la investigación con *Big Data*, así como las funciones que deben desempeñar los comités de ética de la investigación en la evaluación de este tipo de estudios.

Research with Big Data technology in the world of health must be carried out within an ethical and legal framework that guarantees the highest level of protection in the processing of personal data. The research ethics committees, as guarantors of the rights, safety and welfare of the subjects participating in a biomedical research project, must verify compliance with the ethical and legal principles applicable to research with health data. In this paper, we review the ethical and legal principles applicable to research with Big Data, as well as the functions that the research ethics committees must perform in the evaluation of this type of studies.

Palabras clave / Keywords:

Datos de salud / Grandes bases de datos / Comités de ética de la investigación / Principios éticos / Consentimiento informado.

Health Data / Big Data / Research Ethics Committees / Ethical Principles / Informed Consent.

1. Introducción

La utilización de la tecnología *Big Data* en el ámbito de la salud supone nuevas oportunidades para el diagnóstico y el tratamiento de multitud de enfermedades, mediante la incorparación de modelos predictivos encaminados a lograr una asistencia sanitaria más eficiente[1]. En cuanto a la investigación, la aplicación de esta tecnología permite manejar grandes cantidades de datos compartidos, facilitando la verificación de los resultados, su transparencia y

[1] Menasalvas, E. / Gonzalo-Martín, C. / Rodríguez-González, A. "Big Data en salud: retos y oportunidades", *Economía Industrial*, Vol. 405, 2017, pp. 87-97.

reproducibilidad y permitiendo obtener la potencia estadística suficiente para analizar resultados infrecuentes[2].

Sin embargo, el aprovechamiento y la explotación de los datos de salud puede tener efectos claramente negativos, como la fuerte amenaza para la intimidad del paciente que los ha suministrado o de quien se ha extraido la información.

En general, la investigación con tecnología *Big Data* utiliza datos anonimizados. Sin embargo, el avance tecnológico podría llevar a la reidentificación de los datos anonimizados, implicando un riesgo potencial para la privacidad[3]. Otra posible amenaza radicaría en la obtención de datos masivos con un fin autorizado legítimo pero que posteriormente pudieran cederse para usos secundarios no supervisados. A su vez, también es motivo de preocupación la transferencia de datos anonimizados a países con legislaciones menos restrictivas o incluso la cesión de datos a empresas con intereses comerciales. Por último, la utilización de estos datos anónimos puede tener también implicaciones éticas en cuanto a la posibilidad de estigmatizar a grupos sociales o étnicos desfavorecidos, en función del diseño o de los resultados de la investigación. Al hilo de las consideraciones descritas, antes de iniciar cualquier proyecto de investigación deben abordarse de forma exhaustiva los riesgos cuya realización pudiera implicar.

Es necesario hacer hincapié en la importancia de la investigación en biomedicina y en ciencias de la salud, como instrumento clave para avanzar en el conocimiento científico; pero esta investigación sólo puede realizarse si se garantiza la protección de los sujetos participantes. La preocupación por esta protección ha dado lugar, a lo largo de la historia, a los diferentes códigos éticos que han servido de referencia tanto para la comunidad científica como para los comités éticos.

La legislación y las diferentes referencias éticas internacionales asignan a los comités de ética de la investigación (CEI) la función de velar por los derechos, seguridad y bienestar de los sujetos que participan en un proyecto de investigación biomédica. Los CEI deben ser independientes de los patroci-

---

[2] Hemingway, H. / Asselbergs, F.W. / Danesh, J. / Dobson, R. / Maniadakis, N. / Maggioni, A. *et ál*. "Big data from electronic health records for early and late translational cardiovascular research: challenges and potential", *European Heart Journal*, Núm. 16, Vol. 39, 2017, pp. 1481-95.

[3] Opinion 05/2014 on Anonymisation Techniques. Article 29 Data Protection Working Party. European Commission - Justice - Data Protection ; 2014 [Documento en línea; consultado 29/02/2019]. Disponible en: https://ec.europa.eu/justice/article-29/documentation

nadores, financiadores, investigadores, y no deben estar sometidos a ninguna influencia indebida (p. ej. política, institucional, profesional o comercial). De esta forma se garantiza que el interés de los participantes en la investigación sea primordial.

La legislación vigente, o incluso las referencias éticas internacionales, como la Declaración de Helsinki, no hacen referencia a los proyectos de investigación realizados con datos anónimos o anonimizados[4]. No obstante, teniendo en cuenta los riesgos potenciales, incluyendo la posibilidad de reidentificar los datos, es esencial garantizar la protección de los derechos de las personas de quienes proceden, mediante una revisión ética de los proyectos de investigación con tecnologías Big Data, que pondere tanto los posibles beneficios para la sociedad como los riesgos teóricos para los sujetos[5].

Por otra parte, uno de los aspectos cruciales que debe tenerse en consideración es que el manejo de la ingente cantidad de información en la tecnología Big Data hace impracticable la obtención del consentimiento informado de los sujetos, siendo éste uno de los principales aspectos que deben revisar los comités en la evaluación de estos estudios.

El objetivo de esta revisión es analizar los principios éticos y legales aplicables a la investigación con Big Data, así como las funciones que deben desempeñar los comités de ética de la Investigación en la evaluación de este tipo de estudios.

2. Control ético

Cualquier investigación realizada con seres humanos debe estar justificada desde el punto de vista ético, lo que implica que el posible beneficio que se obtenga, para los sujetos participantes o para la sociedad en su conjunto, compense las molestias y/o riesgos derivados de la participación. A su vez, debe respetar los principios éticos universalmente reconocidos, en particular los principios de autonomía, beneficencia, no maleficencia y justicia, por cuyo cumplimiento deben velar los comités de ética de la investigación.

---

[4] Declaración de Helsinki de la AMM – Principios éticos para las investigaciones médicas en seres humanos. Asociación Médica Mundial. [En línea, consultado el 28/04/2019]. Disponible en: https://www.wma.net/es/

[5] CIOMS (Council for International Organizations of Medical Sciences). International ethical guidelines for health-related research involving humans. [En línea; consultado el 28/04/2019]. Disponible en: https://cioms.ch/wp-content

2.1. Principios éticos[6]

El principio de respeto por las personas tiene dos traducciones importantes. Por un lado, el respeto a la autonomía reconoce la capacidad de una persona de tomar decisiones sobre los asuntos que le afectan. En la investigación biomédica, el principio de autonomía es ejercido en particular por el proceso del consentimiento libre e informado, el cual puede ser retirado en cualquier momento sin perjuicio para el sujeto. Por otra parte, este principio se manifiesta también en la protección de las personas con autonomía limitada que participan en proyectos de investigación.

Un principio sustancial, estrechamente relacionado con el de autonomía y que reviste particular importancia para la investigación biomédica, es el de confidencialidad, es decir, que el acceso, control, y difusión de la información personal, recogida con fines de investigación o resultante de la misma, estén resguardados frente a una posible revelación inadecuada.

Los principios de beneficencia y no maleficencia se unen en la obligación moral de maximizar los beneficios posibles y minimizar los potenciales perjuicios para los sujetos que participan en una investigación. El principio de beneficencia tiene implicaciones adicionales, en particular que el diseño del proyecto de investigación sea sólido y cumpla con los criterios aceptados de calidad científica. Este principio hace referencia, además, a que los investigadores tengan la competencia necesaria para realizar la investigación y que se asegure la protección apropiada de los participantes en la misma. Todos los proyectos de investigación deben someterse a una cuidadosa ponderación del balance riesgo/beneficio, lo que implica que sólo deberían llevarse a cabo si los riesgos previsibles y cargas no son desproporcionados frente a los beneficios potenciales. Este balance debe ser especialmente cuidadoso en las investigaciones con personas incapaces de consentir, en particular si la investigación no ofrece ningún beneficio directo potencial a los participantes.

En la investigación que utiliza datos masivos los posibles perjuicios para los sujetos están relacionados con el derecho a la confidencialidad en el manejo de la información, especialmente cuando se traten datos especialmente

[6] The Belmont Report, Ethical Principles and Guidelines for the Protection of Human Subjects of Research. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Office for Human Research Protections. U.S. Department of Health and Human Services; 1979. [En línea, consultado el 29/02/2019]. Disponible en: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

protegidos. No se debe olvidar las posibles repercusiones legales, laborales o personales de una posible revelación de datos personales no autorizada.

El principio de justicia engloba la imparcialidad y la equidad. En la investigación biomédica con seres humanos significa que la distribución de riesgos y cargas que conlleva y el posible beneficio que puede obtener sea justo, un principio conocido como justicia distributiva. Este principio presenta especial relevancia en la investigación realizada en países con recursos muy limitados, así como en la investigación con poblaciones vulnerables. Tal investigación debería ser sensible a las necesidades de salud relevantes para los países/poblaciones involucrados, de modo que tuvieran la posibilidad de beneficiarse de los resultados y de las posibles aplicaciones de la investigación.

En el ámbito de la investigación con tecnología de grandes bases de datos es especialmente importante la protección de los grupos sociales vulnerables, menos conscientes de las consecuencias que puede tener el manejo de sus datos. Por otra parte, debe contemplarse la posible estigmatización de grupos desfavorecidos en función de los resultados que se obtengan en la investigación. También adquiere importancia, en este tipo de investigación, el considerar la aplicación de estos principios éticos teniendo en cuenta las diferencias culturales y legales que puede haber entre los diferentes países[7].

2.2. Recomendaciones internacionales

Teniendo en cuenta el impacto global que pueden tener las tecnologías de análisis de Big Data sanitario y las diversas fuentes de datos disponibles, la revisión ética de estos estudios debería tener en cuenta las diferentes recomendaciones internacionales sobre ética biomédica, tales como la Declaración de Helsinki de la Asociación Médica Mundial[8], las Guías éticas internacionales para investigación biomédica con seres humanos del Consejo de Organizaciones Internacionales de Ciencias Médicas (CIOMS)[7] o la Declaración Universal sobre bioética y derechos humanos, aprobada por la UNESCO[9].

---

[7] CIOMS (Council for International Organizations of Medical Sciences). International ethical guidelines for health-related research involving humans. [En línea; consultado el 28/04/2019]. Disponible en: https://cioms.ch/wp-content

[8] Declaración de Helsinki de la AMM - Principios éticos para las investigaciones médicas en seres humanos. Asociación Médica Mundial. [En línea, consultado el 28/04/2019]. Disponible en: https://www.wma.net/es/

[9] Declaración Internacional sobre Bioética y Derechos Humanos. UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura); 2005 [En línea, consultado el 28/04/2019]. Disponible en: http://portal.unesco.org/es

A su vez, los principios éticos se recogen también en acuerdos legalmente vinculantes para la protección de los participantes en investigación biomédica, como el Convenio de Derechos Humanos y Biomedicina del Consejo de Europa, ratificado por España junto con sus Protocolos Adicionales[10].

Se resumen a continuación las guías éticas cuyo contenido puede tener mayor implicación en el control ético de los estudios objeto de esta revisión.

2.2.1. Declaración de Helsinki de la Asociación Médica Mundial

La exigencia de una evaluación externa e independiente de la investigación biomédica está recogida en los principios éticos para las investigaciones médicas en seres humanos, de la Declaración de Helsinki, promovida por la Asociación Médica Mundial (AMM), cuya revisión de 2013 establece que cualquier proyecto de investigación médica en seres humanos, incluida la investigación que utilice material o datos humanos identificables, debe ser aprobada por un comité de ética de investigación.

La Declaración de Helsinki es el referente ético internacional en investigación biomédica en el que se basa gran parte de la legislación internacional. Establece los principios éticos para la investigación médica en seres humanos, incluida la importancia de proteger la dignidad, autonomía, privacidad y confidencialidad de los participantes en la investigación. Esta Declaración afirma que toda investigación tiene que reflejarse en un protocolo que debe aprobar un comité de ética de investigación antes de comenzar el estudio. Especifica, a su vez, que en toda investigación médica que utilice datos o material de origen humano identificables, el médico debe obtener el consentimiento para la recogida, almacenamiento y/o reutilización. La Declaración plantea que, de forma excepcional, cuando el consentimiento sea imposible o impracticable, la investigación pueda llevarse a cabo sin el consentimiento de los sujetos, únicamente tras ser evaluada y aprobada por un CEI.

Sin embargo, esta Declaración no hace referencia a la investigación realizada con datos anónimos o anonimizados ni a la investigación con tecnologías de análisis de datos masivos.

---

[10] Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997. BOE nº 251, de 20 de octubre de 1999, 36825-30.

2.2.2 .Declaración sobre las consideraciones éticas de las bases de datos de salud y los biobancos de la AMM

La AMM revisó en 2016 la Declaración sobre las consideraciones éticas de las bases de datos de salud y los biobancos, adoptada en 2002[11], afirmando que la recogida y el uso de información de las personas, al margen de la asistencia, debe ser voluntaria y con un consentimiento específico si se recoge expresamente para un proyecto de investigación. La Declaración añade que, cuando la información se almacena en una base de datos para usos múltiples e indefinidos, el consentimiento de los sujetos sólo será válido si han sido informados adecuadamente de los siguientes aspectos: el objetivo de la base de datos y el tipo de información que se recoge; el procedimiento para informar de los resultados; las reglas de acceso a los datos y cómo se protege la privacidad; que si esta información se anonimiza la persona no podrá saber qué se hace con su información ni retirar su consentimiento; las reglas de administración de la base de datos; cuando proceda, la generación de beneficios comerciales, propiedad intelectual y la transferencia de información a otras instituciones o a terceros países.

En esta Declaración se profundiza en algunos aspectos éticos como el derecho del paciente a saber si su información se almacena en una base de datos y los fines para los que se puede utilizar. También establece la obligatoriedad del consentimiento informado de los pacientes si su información se revela a terceros o si acceden a la información personas que no participan en la asistencia, a menos que existan circunstancias excepcionales que lo justifiquen. Estas excepciones consisten en que la base de datos resulte de una exigencia legal o en aquellas situaciones en las que un comité independiente de revisión ética, nombrado especialmente, otorgue su aprobación. En estos casos excepcionales, la Declaración establece que se debe comunicar a los pacientes el uso potencial de su información, incluso si no tienen derecho a oponerse.

Por otra parte, la Declaración de la AMM afirma que debe garantizarse el cumplimiento de los siguientes principios éticos en la administración de las bases de datos de salud:

- Protección de las personas: los derechos de las personas deben predominar sobre los intereses de la ciencia o de otras partes interesadas.

[11] Declaración sobre las consideraciones eticas de las bases de datos de salud y los biobancos. Asociación Médica Mundial. Taipei, Taiwán, octubre 2016. [En línea, consultado el 28/04/2019]. Disponible en: https://www.wma.net/es/

- Transparencia: toda la información pertinente debe estar a disposición del público.

- Participación e inclusión: los responsables de las bases de datos de salud deben consultar y comprometerse con las personas participantes y sus comunidades.

- Responsabilidad: Los responsables de las bases de datos de salud deben ser accesibles y receptivos para los interesados

Para velar por el cumplimiento de estos principios la Declaración establece que un comité de ética independiente debe aprobar la creación de bases de datos de salud utilizadas para investigación, además de evaluar cualquier uso de información y revisar los términos en los que se otorgó el consentimiento, o si se deben adoptar otras medidas para proteger al donante, además del derecho del comité a supervisar cualquier actividad en curso.

La Declaración recoge los derechos que asisten a los sujetos respecto a la información incluida, el derecho a retirar el consentimiento y la información identificable de la base de datos de salud, así como el derecho a solicitar y recibir información sobre sus datos y su uso. Contempla que, en situaciones de amenaza grave para la salud de la población en las que la información anónima no sea suficiente, un comité de ética podría confirmar la excepción al consentimiento.

Por último, la Declaración establece una serie de aspectos que deben ser contemplados en la administración de una base de datos de salud, que deberían ser evaluados por el comité de ética independiente responsable de su aprobación. Estos aspectos son los siguientes: el objetivo de la base de datos y naturaleza de la información incluida; los usos previstos de los datos, incluyendo posibles actividades comerciales; las condiciones y duración del almacenamiento y disposiciones sobre la eliminación de la información; la trazabilidad de la información, de acuerdo con el consentimiento que se ha otorgado; el manejo de la información en caso de cambio de responsable o cierre; el método para obtener y registrar un consentimiento apropiado, u otra base legal para recopilar la información; las medidas para proteger la dignidad, autonomía, privacidad y evitar la discriminación; los criterios y procedimientos sobre el acceso y el intercambio de información, incluyendo los acuerdos de transferencia de datos, si fuera necesario; las medidas de seguridad para evitar accesos no autorizados o intercambios inapropiados; los procedimientos para volver a contactar a los participantes cuando sea

pertinente; los procedimientos para recibir y realizar preguntas y quejas y las personas responsables de administrar la base de datos.

Sin embargo, esta Declaración no trata de forma directa la investigación realizada con datos anonimizados utilizando la tecnología de análisis masivo de datos. Tampoco hace referencia a la posibilidad de reidentificar datos anonimizados, principal preocupación de la investigación con *Big Data* sanitario. Esta declaración incluye también a las muestras biológicas y la información biológica o genética que se pueda obtener de ellas[12].

2.2.3. Pautas éticas internacionales para la investigación relacionada con la salud en seres humanos del Consejo de Organizaciones Internacionales de las Ciencias Médicas (CIOMS) en colaboración con la Organización Mundial de la Salud (OMS)[13]

Estas pautas éticas, revisadas en el año 2016, se dirigen a todas las categorías de investigación relacionada con la salud. El documento hace referencia, en varios de sus apartados, al manejo de datos con fines de investigación, e incluso dedica unas pautas específicas a la utilización de datos obtenidos en la red y a la utilización de herramientas digitales en investigación. A continuación, se destacan las pautas más relevantes para el objetivo de esta revisión:

a. Pauta 12. Utilización de datos en la investigación relacionada con la salud

Cuando se almacenen datos las instituciones responsables de la custodia deben establecer cómo se va a obtener la autorización para el uso futuro con fines de investigación, garantizando el respeto a los derechos y el bienestar de los sujetos fuente de los datos. Para ello, deben disponer de un sistema de gobierno en el que se especifiquen al menos los siguientes apartados:

- A qué entidad legal se encomiendan los datos;

[12] Nicolás, P., Voz "Dato genético", *Enciclopedia de Bioderecho y Bioética,* Romeo Casabona, C. (Dir.) Ed. Cátedra Interuniversitaria de Derecho y Genoma Humano – Ed. Comares y Fundación Instituto Roche, Bilbao-Granada, 2016. [En línea, consultado el 28/04/2019]. Disponible en: https://enciclopedia-bioderecho.com/voces/92

[13] CIOMS (Council for International Organizations of Medical Sciences). International ethical guidelines for health-related research involving humans. [En línea; consultado el 28/04/2019]. Disponible en: https://cioms.ch/wp-content

- Cómo se obtiene la autorización del sujeto fuente, cómo se ejerce el derecho de revocación y en qué circunstancias se debe contactar de nuevo con el sujeto;

- Un procedimiento para determinar si deberían revelarse los hallazgos inesperados y si es así, cómo debería gestionarse;

- Cómo se controla la calidad de los datos;

- Cómo se mantiene la confidencialidad del vínculo entre los datos recogidos y los identificadores personales de los sujetos;

- Quién puede acceder a los datos para futuras investigaciones y en qué circunstancias;

- Qué organismo podría revisar las propuestas de investigación para usos futuros de los datos;

- Mecanismos apropiados para informar a los sujetos de los resultados de la investigación;

- Cómo se organiza el compromiso de participación de grupos de pacientes o la comunidad;

- Con qué otras fuentes de información personal se cruzan los resultados de los análisis de datos;

- Los tipos de investigación que se van a llevar a cabo y los que se excluyen, o aquellos que se realizarán únicamente contactando de nuevo con el sujeto para obtener el consentimiento;

- A quién corresponden los beneficios obtenidos de la investigación;

- Cómo se preservan los derechos y el bienestar de los sujetos participantes.

Cuando los datos se obtienen y almacenan con fines de investigación se debe obtener el consentimiento del sujeto de quien se obtienen los datos, bien específico para un uso particular o bien amplio para futuros usos no especificados. La aceptabilidad ética de los consentimientos amplios

depende de que el registro de datos cuente con procedimientos de gobierno adecuados.

Cuando se usan datos recogidos en el contexto de la atención clínica de rutina debería ponerse en marcha un procedimiento para que los participantes puedan optar de manera informada a no ser incluidos, de forma que los datos puedan almacenarse y usarse para investigación salvo que la persona haya manifestado de manera explícita su objeción. Sin embargo, esta objeción no se aplicaría cuando sea obligatorio incluir datos en registros de población. El procedimiento para solicitar no ser incluido debe cumplir las siguientes condiciones: 1) los pacientes deben estar al tanto de su existencia; 2) debe suministrarse información suficiente; 3) debe informarse sobre la opción de retirar sus datos; y 4) debe ofrecerse una posibilidad genuina de negarse.

Cuando los investigadores quieran usar datos almacenados, procedentes de investigaciones anteriores, de la asistencia o de otras fuentes, sin haber obtenido el consentimiento para su uso futuro en investigación, un comité de ética de la investigación podría considerar la exención del consentimiento individual cuando: a) la investigación no pudiera realizarse sin dicha exención; b) la investigación tenga un valor social importante; c) la investigación no suponga más que riesgos mínimos a los participantes o al grupo al que pertenecen.

Las Pautas establecen que se debe asegurar la confidencialidad de la información asociada a los datos, compartiendo con los investigadores sólo información anonimizada o codificada y limitando el acceso a terceros. La identificación de los sujetos debe permanecer en poder del responsable de la custodia de los datos.

La pauta nº 12 recuerda que los datos de entornos desfavorecidos deberían recogerse y almacenarse únicamente en colaboración con las autoridades sanitarias locales. La estructura de gobierno de la base de datos debería tener representación de la comunidad de la que proceden los datos y compartir con ella los resultados y beneficios.

Las Pautas éticas recomiendan que cualquier estudio que utilice datos almacenados se remita a un comité de ética de la investigación, que debe revisar si el uso propuesto de los datos corresponde con lo autorizado previamente por el sujeto, especialmente si otorgó un consentimiento amplio para la utilización de datos. Si el uso propuesto estuviera fuera del

alcance autorizado para la investigación será necesario solicitar un nuevo consentimiento.

Las pautas establecen que, para los registros poblacionales obligatorios, el análisis interno del registro puede quedar exento de revisión por el comité conforme a las disposiciones legales. Por otra parte, el investigador debería obtener un consentimiento informado explícito en las siguientes circunstancias: si la investigación implica riesgos superiores al mínimo para el sujeto; se utilizan técnicas controvertidas o de alto impacto, aunque estén aprobadas y si la investigación se desarrolla en entornos de alta vulnerabilidad.

De especial interés es el comentario a esta pauta titulado "límites de la confidencialidad", en el que se reconoce que los sujetos deberían estar informados de la creciente dificultad para asegurar una confidencialidad absoluta y de las posibles consecuencias adversas de una revelación de datos. Se argumentan tres razones principales: 1) incluso con una buena estructura de gobierno de la base de datos existe la posibilidad de que haya filtraciones o sustracciones de datos y lleguen a terceros no autorizados; 2) los avances tecnológicos permiten que los datos de diferentes fuentes se puedan cruzar y que datos inicialmente anonimizados o codificados se puedan reidentificar por los investigadores o por terceros, en especial en investigaciones de ámbitos restringidos (procedentes de un centro pequeño) o específicos (como el caso de enfermedades raras); en estos casos, utilizar datos agregados de fuentes similares puede disminuir la posibilidad de reidentificación. Por otra parte, la información genética permite identificar, de forma cada vez más precisa, a los individuos; 3) la declaración de información confidencial puede ser un requisito legal como en el caso de conductas delictivas o enfermedades de declaración obligatoria. Del mismo modo, las autoridades y los comités de ética de la investigación pueden tener acceso legal a inspeccionar los archivos de un proyecto de investigación, al igual que los monitores de un estudio por cuenta del promotor. Estas posibles limitaciones para mantener la confidencialidad deberían ponerse en conocimiento de los potenciales participantes en una investigación.

Por último, las pautas establecen que la utilización de datos identificados para una investigación debería ser excepcional, y en esos casos los investigadores deberán explicar al comité ético de investigación por qué es necesario conservar los identificativos y cómo se va a proteger la confidencialidad.

b. Pauta 22. Uso de obtenidos en la red y herramientas digitales en la investigación relacionada con la salud:

Las Guías CIOMS, en los comentarios de la Pauta 22, señalan las nuevas oportunidades que generan para la investigación las tecnologías de la información y comunicación, tanto internet como las redes sociales. Sin embargo, las características de estos entornos plantean un gran reto para la protección de la privacidad de las personas. Actualmente los usuarios comparten información personal y de su entorno cercano en la red con gran número de personas. Esta información compartida supone una gran cantidad de datos que puede analizarse por entidades públicas o privadas mediante herramientas de extracción automática y pueden llegar a tener un valor comercial importante.

La Pauta 22 especifica que, cuando los investigadores utilicen herramientas en línea y digitales para obtener datos en investigaciones relacionadas con la salud, deberían disponer de medidas para proteger a los individuos de la posible revelación de sus datos o de la reidentificación, cuando las bases de datos se publiquen, compartan, se combinen o se crucen con otras bases de datos. Los investigadores deberían valorar los riesgos para la privacidad en la investigación y reducirlos en la medida de lo posible.

Los investigadores deben reflejar en el protocolo cómo se van a tratar los datos obtenidos en plataformas en línea, junto con los riesgos potenciales para la privacidad y qué se hace para mitigarlos. La existencia de datos e información disponible en la red no exonera a los investigadores de la obligación de respetar la privacidad y reducir los riesgos que podrían resultar de combinar datos de múltiples fuentes y su uso y publicación posterior. Por este motivo, ante el riesgo de revelación no autorizada o inadvertida junto con la aparición de tecnologías que aumentan la cantidad y el tipo de datos identificables, se remarca la necesidad de reforzar la seguridad de los datos y la protección de la privacidad en este contexto. Es especialmente importante tratar los riesgos potenciales de grupos vulnerables, que podrían verse perjudicados como resultado de la revelación de información.

Los investigadores deberían informar a las personas cuyos datos se recogen en investigaciones "en línea" de los siguientes aspectos: la finalidad y el contexto del uso previsto de la información, las medidas de privacidad y seguridad adoptadas para proteger sus datos y las limitaciones de estas medidas. Por otra parte, los investigadores no deberían utilizar los datos de los sujetos que se nieguen a participar y se deberían establecer procedimientos de revocación y cancelación. El procedimiento de revocación debería cumplir los requisitos mencionados en la Pauta 12.

Respecto a la evaluación de los riesgos para la privacidad, los comentarios a la Pauta 22 señalan que debería abarcar las potenciales amenazas para la privacidad, los aspectos que aumentan estos riesgos, la probabilidad de que haya una revelación de información teniendo en cuenta estas amenazas y el alcance, la gravedad y la probabilidad de los riesgos que surgen de las posibles revelaciones.

Algunos riesgos son difíciles de prever dado que los datos se acumulan, combinan y se usan en una gran variedad de contextos, como el uso cada vez más frecuente de teléfonos móviles para investigaciones sobre intervenciones clínicas o de salud pública. La comodidad y la accesibilidad de los dispositivos móviles para usuarios o investigadores permiten la recogida y la rápida transmisión de datos en una variedad de entornos. Los investigadores que utilicen dispositivos móviles y aplicaciones para recoger datos deben tener en cuenta que estas herramientas pueden tener características y limitaciones muy diferentes en relación con la privacidad.

Los riesgos para la privacidad no son un simple resultado de la presencia o ausencia de determinados campos, atributos o palabras clave en un conjunto de datos. Gran parte del riesgo potencial para la privacidad surge de lo que se puede inferir acerca de los individuos, a partir de los datos en su conjunto, o cuando éstos se cruzan con otra información disponible. Las aproximaciones habituales a la protección de datos a menudo proporcionan protección limitada. Las técnicas tradicionales de desidentificación tienen importantes limitaciones y unos pocos datos pueden ser capaces de identificar inequívocamente a un individuo en un conjunto de datos[14].

Las Guías explican que es esencial que los investigadores seleccionen y pongan en práctica medidas apropiadas para reducir los riesgos para la privacidad, teniendo en cuenta los usos previstos y los riesgos asociados a los datos. Estas medidas a su vez requieren un análisis sistemático de los usos primarios y secundarios de los datos, considerando los riesgos de reidentificación y los riesgos asociados a la posible inferencia de datos. Este análisis debería tener en cuenta no sólo si una persona puede asociarse directamente con una característica particular, sino además los usos potenciales de los datos o los fines previstos del análisis.

Los investigadores deberían identificar y gestionar los riesgos durante la recogida, el procesamiento y la difusión de los datos. Las consideraciones

[14] Weeney L., *Simple demographics often identify people uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3. 2000.

sobre la privacidad requieren un enfoque especialmente cauteloso cuando se trata de diseminar datos en Internet. Las publicaciones académicas y algunas instituciones a menudo requieren que los investigadores hagan públicos los resultados, en ocasiones en un formato de datos abierto. La divulgación pública en tales formatos puede ser problemática para los conjuntos de datos que permitan la reidentificación de los sujetos. Una vez que se publica un conjunto de datos en la red, el investigador pierde el control sobre los usos posteriores.

Sin embargo, a pesar del valor como referentes éticos que tienen estas Declaraciones, se trata de recomendaciones sin validez legal.

3. Marco normativo

3.1. Ley 14/2007, de 3 de julio, de Investigación biomédica

La Ley 14/2007, de 3 de julio, de Investigación biomédica (LIB) estableció un marco regulador específico en España, con objeto de garantizar la realización de una investigación con pleno respeto a la dignidad e identidad humanas y a los derechos inherentes a las personas que participan en la investigación. Esta Ley establece que la autorización y desarrollo de cualquier proyecto de investigación sobre seres humanos o su material biológico requiere el previo y preceptivo informe del comité de ética de la investigación. La LIB creó estos comités como instrumentos fundamentales para garantizar la evaluación y seguimiento de los proyectos de investigación, definiendo las funciones que deben desempeñar. Posteriormente, el 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, definió "Comité de Ética de la Investigación" como "órgano independiente y de composición multidisciplinar cuya finalidad principal es la de velar por la protección de los derechos, seguridad y bienestar de los sujetos que participen en un proyecto de investigación biomédica y ofrecer garantía pública al respecto, mediante un dictamen sobre la documentación correspondiente del proyecto de investigación, teniendo en cuenta los puntos de vista de las personas legas, en particular, los pacientes, o las organizaciones de pacientes".

Debe tenerse en cuenta que la investigación con tecnología *Big Data* es generalmente observacional. En este sentido es fundamental resaltar que, si bien es cierto que la LIB, en el art. 2, estableció que "la autorización

y desarrollo de cualquier proyecto de investigación sobre seres humanos o su material biológico requerirá el previo y preceptivo informe favorable del comité de ética de la investigación", en su preámbulo excluyó expresamente de su ámbito de actuación los estudios observacionales, reconociendo a la Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LAP) y a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), su condición supletoria en aquellas cuestiones no reguladas por esta Ley.

3.2. La Ley de Autonomía del Paciente

La LAP regula la utilización de la historia clínica, garantizando su fin principal, que es facilitar una asistencia sanitaria adecuada. Esta Ley autoriza el acceso a la historia clínica a los profesionales sanitarios sin el consentimiento del sujeto cuando sea necesario para la asistencia. También autoriza el acceso sin consentimiento para otros usos relacionados directamente con la asistencia, concretamente para el personal sanitario "que ejerza funciones de inspección, evaluación, acreditación y planificación", con el fin de "comprobar la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios". La ley 33/2011, General de Salud Pública, añadió una tercera excepción al consentimiento cuando fuera necesario para prevenir riesgos para la salud de la población.

En cuanto al acceso a la historia clínica con fines de investigación, la LAP se remitía a lo dispuesto en la LOPD, estableciendo que "el acceso a la historia clínica con fines de investigación obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos".

La LOPD ha sido derogada tras la reciente publicación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos (LOPD-GDD), que en su Disposición final novena, ha contemplado una nueva habilitación legal para acceder a la historia clínica con fines de investigación biomédica, añadiendo el siguiente párrafo al literal referido en el párrafo anterior:

> "Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición Adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales".

A pesar de la introducción de este nuevo párrafo el enunciado original de la Ley de Autonomía del Paciente no se ha modificado, por lo que la redacción de los términos en los que se puede acceder a la historia clínica sigue siendo confusa. Así, no queda claro si este nuevo párrafo permite el acceso a la historia clinica para investigación con los datos de identificación personal del paciente, si habilita la forma en que se extraen los datos de la historia (anonimizados, seudonimizados o codificados o identificados) o si, por el contrario, permite acceder a la historia clínica para investigación sin el consentimiento del sujeto con las garantías adicionales de la Disposición adicional decimoséptima de la LOPD-GDD. En este sentido, sería conveniente disponer de informes jurídicos de la AEPD que clarificasen estas cuestiones, en línea con un reciente informe de la Autoridad Catalana de Protección de Datos sobre este tema[15].

3.5. Reglamento Europeo de protección de datos

El Reglamento Europeo de protección de datos (RGPD), que entró en vigor el 25 de mayo de 2018, establece requisitos específicos a los tratamientos de datos de salud, considerados como categorías especiales, permitiendo su tratamiento únicamente con unas garantías reforzadas. Este Reglamento reconoce la importancia que tiene la investigación científica con datos de carácter personal.

En su considerando 26 hace referencia a que "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

Este considerando también establece que los datos personales seudonimizados, es decir, los datos que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.

[15] Dictamen CNS 15/2019 Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomédica. Autoridad Catalana de Protección de Datos. [En línea, consultado el 28/06/2019] Disponible en https://apdcat.gencat.cat/es/

El RGPD no hace referencia a la utilización de tecnología *Big Data*; no obstante, el considerando 91 cita "las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional, y que podrían afectar a un gran número de interesados y entrañen probablemente alto riesgo, por ejemplo, debido a su sensibilidad". En tales casos, el RGPD establece que "el responsable debe llevar a cabo antes del tratamiento, una evaluación de impacto relativa a la protección de datos" que "debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento".

3.5.1. Implicaciones del Reglamento Europeo de proteccion de datos en la investigación

El Reglamento Europeo de protección de datos (RGPD) establece que el tratamiento con fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales; tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines.

El Reglamento define un nuevo tipo de tratamiento de datos, denominado "seudonimización", como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

En lo referente a aspectos de seguridad, además del cumplimiento del principio de minimización de datos, el RGPD incorpora importantes novedades, como la introducción temprana en las organizaciones de políticas de privacidad de los datos, la evaluación previa del impacto de los tratamientos planificados, la adopción de medidas de seguridad, el mantenimiento de un registro de actividades de tratamientos, el nombramiento de un delegado de protección de datos, la elaboración de códigos de conducta y esquemas de certificación, la obligatoriedad de la consulta a las autoridades de control en los casos en los que la evaluación del impacto determina un alto riesgo

y la notificación de los incidentes y brechas de seguridad. Se desarrollan a continuación varios conceptos que incorpora esta normativa:

3.5.2. Responsabilidad activa y gestión de riesgos

El cambio principal introducido en el Reglamento es la evolución de un modelo basado en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una valoración previa por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan. El reglamento define «responsable del tratamiento» como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento y «encargado del tratamiento» como la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento.

El responsable o el encargado del tratamiento deben mantener registros de las actividades de tratamiento bajo su responsabilidad, estando obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros de modo que puedan servir para supervisar las operaciones de tratamiento.

3.5.3. Protección desde el diseño y por defecto

El Reglamento exige que el responsable del tratamiento adopte políticas internas y aplique medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

El art. 25 del RGPD describe la protección de datos desde el diseño como la obligación del responsable del tratamiento de aplicar, tanto en el momento de determinar los medios para el tratamiento, como durante el mismo, las medidas técnicas u organizativas adecuadas, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

En cuanto a la obligación de la protección de datos por defecto, señala el art. 25 que "el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo

sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". El considerando 78 del RGPD especifica que las medidas técnicas y organizativas referidas "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".

Por otra parte, el Reglamento exige el cumplimiento del principio de minimización de datos, es decir que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. En este sentido, deberán definirse los datos que se van a utilizar, la extensión del tratamiento, el tiempo y lugar de almacenamiento, el responsable del tratamiento y los fines previstos.

3.5.4. Evaluacion de impacto

La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado deben ponderarse sobre la base de una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo y, en su caso, si dicho riesgo es alto. En tales casos, el Reglamento prevé que el responsable debe llevar a cabo antes del tratamiento una evaluación de impacto relativa a la protección de datos (EIPD) con el fin de valorar la particular gravedad y probabilidad de riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el Reglamento.

El RGPD establece que, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos semejantes.

La EIPD es una herramienta con carácter preventivo, que debe realizar el responsable del tratamiento, para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con objeto

de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el fin de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable. Esta evaluación deberá incluir como mínimo[16]:

- Una descripción sistemática de la actividad de tratamiento prevista.
- Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.
- Una evaluación de los riesgos.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

En este sentido, la Agencia Española de Protección de Datos (AEPD) ha publicado recientemente una lista de los tipos de operaciones de tratamiento que requieren una EIPD[17] y del mismo modo, ha establecido otro listado de los tipos de tratamientos que no requieren dicha EIPD[18]. Según este documento, cualquier tratamiento de datos que cumpla dos o más criterios del listado debería considerarse que entraña probablemente un alto riesgo y requeriría una EIPD. Este sería el caso de cualquier tratamiento de datos que implique el uso de datos relacionados con la salud, datos genéticos o datos de sujetos vulnerables o menores, si además cumple el requisito adicional de ser tratamientos que impliquen el uso de datos a gran escala o que impliquen la asociación, combinación o enlace de registros de bases de datos con finalidades o responsables diferentes o que tengan como objeto la elaboración de perfiles.

---

16 Agencia Española de Protección de Datos, *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD*. [En línea, consultado 28/02/2019], Disponible en: www.agpd.es.

17 Agencia Española de Protección de Datos, *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos*. [En línea, consultado 20/09/2019]. Disponible en: https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

18 Agencia Española de Protección de Datos. *Listas orientativa de tipos de tratamientos que no requieren una evaluación del impacto relativa a la protección de datos según el artículo 35.5 del RGPD*. [En línea, consultado 20/09/2019]. Disponible en: https://www.aepd.es/media/guias/ListasDPIA-35.5l.pdf

Estas EIPD pueden realizarse de forma genérica, mediante la adhesión a códigos de conducta por parte de los organismos que agrupen a responsables o encargados del tratamiento, como por ejemplo, los institutos de investigación biomédica o los centros sanitarios. También se podrán poner en marcha sistemas de certificación en materia de protección de datos con objeto de demostrar el cumplimiento de lo dispuesto en el RGPD.

3.5.5. Funciones encomendadas a las instancias encargadas de supervisar los proyectos de tratamientos con datos de salud

El Reglamento considera obligatorio que se designe la figura del delegado de protección de datos (DPD), entre otros, cuando el tratamiento lo lleve a cabo una autoridad u organismo público o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos como por ejemplo los relativos a la salud. El Reglamento prevé que el delegado se ocupe como mínimo de las siguientes cuestiones: informar y asesorar al responsable de las obligaciones derivadas de la normativa aplicable; supervisar el cumplimiento de dicha normativa y de las políticas de protección de datos de la organización, incluida la sensibilización y formación del personal; ofrecer el asesoramiento solicitado en la evaluación de impacto y supervisar su aplicación y cooperar con la autoridad de control.

3.6. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Esta ley (en adelante LOPD-GDD), que deroga la Ley Orgánica 15/1999, de Protección de Datos de Carácter personal, se dicta de conformidad con el Reglamento (UE) 2016/679. Como novedad, en cuanto a su aplicación en la investigación biomédica, la Ley dedica la *Disposición adicional decimoséptima* al tratamiento de datos de salud. Esta disposición establece, en el art. 2, los criterios por los que se debe regir el tratamiento de datos en la investigación en salud:

a) El interesado o, en su caso, su representante legal podrá otorgar el *consentimiento para el uso de sus datos con fines de investigación* en salud y, en particular, la biomédica. Tales finalidades podrán

abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora[19].

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo *estudios científicos sin el consentimiento* de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública[20].

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

En tales casos, los responsables deberán publicar la información, establecida por el artículo 13 del Reglamento Europeo 2016/679, en el que se recoge la información que deberá facilitarse cuando los datos personales se obtengan del interesado[21], en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

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

---

[19] La posibilidad de un consentimiento amplio para investigación es una novedad de esta Ley, al hilo de lo establecido en el RGPD en su considerando 33.

[20] En estos dos primeros tipos de estudio no se hace referencia a la evaluación por un Comité de Ética de la investigación, lo que supone una contradicción con lo dispuesto en el resto de legislación que regula la investigación biomédica o lo establecido en las diferentes recomendaciones internacionales sobre investigación biomédica.

[21] La información que debe proporcionarse, en cumplimiento del artículo 13 del RGPD, corresponde a: la identidad y los datos de contacto del responsable y del delegado de protección de datos, en su caso; los fines del tratamiento; plazo durante el cual se conservarán los datos personales; derecho a solicitar al responsable del tratamiento el acceso a los datos personales, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada o el derecho a presentar una reclamación ante una autoridad de control.

d) Se considera lícito el *uso de datos personales seudonimizados* con fines de investigación en salud y, en particular, biomédica[22]. El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

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

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando: i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación; ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

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

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

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

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

[22] La utilización de datos seudonimizados es un nuevo supuesto que habilita legalmente la utilización de datos relacionados con la salud para investigación biomédica sin el consentimiento de los sujetos fuente siempre que se cumplan una serie de requisitos adicionales. La utilización de datos seudonimizados, en línea con lo establecido por el RGPD, se convierte en el estándar de utilización de datos con fines de investigación biomédica.

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

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

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos[23].

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

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

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

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

[23] Según el literal de la redacción de la LOPD-GDD, los estudios con datos anonimizados también deberían evalurse por un comité de ética de la investigación y realizar, cuando proceda, una EIPD por los riesgos asociados a la reidentificación. En este sentido, se debe recordar que el listado de tratamientos obligados a realizar una EIPD publicada por la AEPD, incluye los tratamientos con datos relativos a la salud que utilicen datos a gran escala, como es el caso de los proyectos que utilicen *Big Data* sanitario.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679[24].

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

Podemos destacar, como cambio relevante introducido en esta nueva Ley, la exigencia de que los estudios observacionales con datos personales sean informados favorablemente por los comités de ética de la investigación, incluyendo los realizados con datos anonimizados.

Por último, la **Disposición Transitoria sexta** de la LOPD-GDD establece el régimen de reutilización, con fines de investigación en materia de salud y biomédica, de datos personales recogidos con anterioridad a la entrada en vigor de esta Ley. Estos requisitos, especificados a continuación, son menos exigentes que los establecidos para los datos recogidos con posterioridad a la entrada en vigor de la Ley: "Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes: a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento; b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial"

Por lo tanto, este enunciado permite realizar estudios con datos recogidos en un estudio previo, pero no hace mención a la evaluación por un comité de ética de la investigación o al deber de informar a los sujetos, como ocurre con los datos obtenidos a partir de la entrada en vigor de esta Ley. Hubiese sido

[24] Es importante destacar que los centros sanitarios en España están tutelados por un CEI. Si los datos se ceden a terceros países debería supervisarse la cesión de datos por un CEI acreditado.

coherente, con el sentido de la Ley, que esta reutilización de datos también requiriera la aprobación de un comité de ética de la investigación.

4. Aspectos adicionales que deben revisar los CEI, en la evaluación de proyectos de investigación, en cumplimiento de las exigencias del nuevo marco normativo en materia de protección de datos

Los CEI, como garantes de los derechos, seguridad y bienestar de los sujetos que participan en una investigación, deben verificar que los estudios sometidos a su consideración cumplen los principios éticos y legales aplicables. Así, deben comprobar que los centros investigadores que tutelan cuentan con el asesoramiento del delegado de protección de datos, y que se dispone de un plan de protección de datos que define los responsables y encargados del tratamiento y la información referente a los registros de las actividades del tratamiento.

Como se ha descrito previamente, la LOPD-GDD atribuye a los CEI la responsabilidad de establecer el control ético de la investigación con datos personales. Si bien es cierto que exige, de forma expícita, el informe del CEI cuando se plantee utilizar con fines de investigación datos seudonimizados, o cuando vayan a reutilizarse datos personales recogidos después de la entrada en vigor de la LOPD-GDD, es importante resaltar el papel que asigna a los CEI en la investigacion con otras categorías de datos. En este sentido, la disposición adicional decimoséptima establece las exigencias de composición de los CEI (DPD o experto en el RGPD), cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Para garantizar el cumplimiento de las exigencias del RGPD/LOPD-GDD los comités deberían coordinarse con las autoridades de control y con el DPD de los centros investigadores y comprobar que, cuando proceda, se ha realizado una evaluación de impacto en la protección de datos personales desde las fases iniciales de cualquier proyecto que trate datos de salud. En este sentido, serían aceptables las evaluaciones de impacto globales, no siendo necesario verificar su realización si la institución donde se desarrolla el proyecto ya los ha acreditado en evaluaciones anteriores. Debe tenerse en cuenta que los proyectos de una misma institución podrán considerarse como un único tratamiento, a no ser que tengan un elemento diferencial que permita afirmar la existencia de nuevos tratamientos.

En relación al cumplimiento de las exigencias del RGPD y de la LOPD-GDD los CEI deben revisar los siguientes aspectos:

– Qué datos se prevé recoger, cumpliendo los principios de protección de datos desde el diseño y por defecto, aplicando el principio de minimización de datos, es decir, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación para los fines de la investigación.

– Que se han aplicado, siempre que sea posible para el desarrollo de la investigación, los procesos de anonimización y/o seudonimización, como herramientas válidas para garantizar la privacidad de los datos personales.

– Que se dispone de controles sobre las condiciones en las que se suministran los datos y sus posibles usos secundarios no consentidos, aspecto fundamental cuando los datos proceden de las historias clínicas.

– Que existe una base legítima para el tratamiento de los datos. Si el tratamiento debe basarse en el consentimiento, que éste se ha prestado en términos adecuados.

– Que el responsable del tratamiento se ha comprometido a aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos de salud es conforme con la legislación.

  Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables deberán determinar de modo transparente y de mutuo acuerdo sus responsabilidades, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información. Dicho acuerdo podrá designar un punto de contacto para los interesados.

– Que el encargado del tratamiento ofrezca suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del RGPD, incluida la seguridad del tratamiento. Si los datos se ceden a un tercero ajeno al centro debe

aportarse un contrato con el encargado de tratamiento; por ejemplo, cuando se contratan empresas para gestionar desplazamientos de pacientes que están participando en un estudio de investigación y se les ceden datos identificativos.

– La adhesión a códigos de conducta o a un mecanismo de certificación, podrá demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento, o del encargado del tratamiento, garantizando la protección de los derechos del interesado.

El CEI debe evaluar la idoneidad de los medios previstos para el tratamiento de los datos y revisar las medidas de seguridad para garantizar la privacidad. Deberá conocer y aprobar las medidas de gobernanza de las bases de datos y registros que se autoricen. El CEI debe revisar la información sobre el servidor en el que se van a alojar los datos y las medidas de seguridad que vayan a adoptarse:

– Será aceptable utilizar servidores que cumplan con un plan de protección de datos; como por ejemplo, las bases de datos alojadas en el servidor del centro sanitario/institución/servicio de salud cuando se ha realizado una EIPD.

– Cuando se utilicen servidores que no dispongan de un plan de protección de datos deberán evaluarse las medidas de seguridad previstas para el tratamiento de los datos. Estas medidas deberán reflejarse tanto en el protocolo, como en el contrato con el encargado del tratamiento.

– Cualquier posible cesión de datos con fines de investigación, además de precisar del consentimiento expreso de las personas afectadas, debe realizarse con conocimiento del tipo de datos que se tratarán, el objetivo del tratamiento, durante cuánto tiempo se van a conservar y tratar y si se van a relacionar o cruzar con otros datos procedentes de diferentes fuentes.

– Garantías de obtención del consentimiento informado. El RGPD y la LOPD-GDD permiten el tratamiento de datos relativos a la salud con fines de investigación científica cuando se cuente con el consentimiento explícito del interesado, que podrá ser amplio para áreas generales vinculadas a una especialidad.

– En el proceso de evaluación del consentimiento informado, los CEI deben revisar que la hoja informativa describe los aspectos más relevantes del derecho de información recogido en el RGPD, explicando quién es el responsable del tratamiento de los datos y ante quién pueden ejercitar sus derechos, es decir ante el investigador principal del estudio o ante el DPD del centro. Los sujetos tienen derecho a recibir la información pertinente en el momento de la recogida de datos, que debe constar al menos de los fines y el contexto de los usos previstos de la información, las medidas de seguridad para proteger la privacidad, los riesgos para la confidencialidad, las limitaciones de las medidas de protección y los riesgos existentes. A su vez, deben recibir información sobre el derecho a conocer quiénes son los destinatarios de sus datos, el plazo de conservación, a quién los pueden ceder, el derecho a solicitar al responsable la suspensión del tratamiento de los datos y el derecho a la rectificación de los datos cuando sean inexactos o estén incompletos.

– Debe permitirse a los interesados dar su *consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación*, en la medida en que lo permita la finalidad perseguida. El CEI deberá revisar si el uso propuesto de los datos en el proyecto de investigación corresponde con lo autorizado previamente por el sujeto, en el caso de haber otorgado un consentimiento amplio para la utilización de los datos.

– El CEI podrá admitir la exención de consentimiento informado cuando se plantee el *uso de datos personales seudonimizados.* En este caso verificará que se dispone de:

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

  o Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación y se hayan adoptado medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

– En cumplimiento de la LOPD-GDD se podrá admitir también la realización de estudios sin consentimiento informado cuando se contemple la reutilización de datos personales con fines de investigación en materia de salud y biomédica. Esta situación se podrá aceptar cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integró científicamente el estudio inicial. En estos casos, los CEI deberán verificar que:

  - el objetivo del estudio esté relacionado con la finalidad o área en la que se enmarcó el estudio inicial.

  - la información sobre el estudio está publicada en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y que se ha notificado la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato. En este sentido las instituciones deben habilitar mecanismos para la difusión de la información sobre los estudios en los que se utilicen estos datos.

Si bien es cierto que, tal y como recoge la disposición transitoria sexta, en el caso en que los datos originales se hubiesen recogido con anterioridad a la entrada en vigor de la LOPD-GDD, no se exige la autorización por un CEI o el derecho de acceso a la información, los derechos de los titulares de los datos deberían ser los mismos con independencia del momento en el que fueron recogidos. De esta manera, tal y como describen las pautas éticas internacionales, la reutilización con fines de investigación en salud y biomédica de datos personales, recogidos lícitamente con anterioridad a la entrada en vigor de esta ley, deberían ser igualmente evaluados por un CEI, garantizando a su vez el derecho del titular de los datos a recibir información sobre el uso de los mismos. Estos derechos están recogidos en la pautas éticas, tal y como se ha especificado previamente en esta revisión; en este sentido, debe resaltarse que el RGPD, en el considerando 33, hace referencia a que deben respetarse las normas éticas reconocidas para la investigación científica.

– Como premisa general, como se ha comentado anteriormente, los CEI deben comprobar que el centro investigador dispone de un plan de gestión de riesgos, incluyendo la realización de una evaluación de impacto. En este sentido, es importante incidir en las garantías adicionales que deben aplicarse en los estudios realizados en población vulnerable. Así, en cumplimiento de las exigencias del art. 28.2 de la LOPD-GDD, los CEI deben verificar si se ha analizado la necesidad de realizar una EIPD cuando se traten datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad. Esta valoración también debe llevarse a cabo cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

– Por otra parte, los comités deben asegurar que se establecen mecanismos para posibilitar el rechazo a la utilización de los datos para investigación y de cancelación, en cumplimiento del art. 21 del RGPD, que establece que "Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público".

– La LOPD-GDD establece que, cuando se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica, se someterá la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. Si bien es cierto que la Buena Práctica Clínica (BPC) engloba una serie de normas dirigidas a garantizar los derechos de los sujetos que participan en un ensayo clínico, su cumplimiento en cualquier tipo de estudio permite asegurar la calidad de los datos y garantizar la fiabilidad de los resultados obtenidos. En este sentido, los CEI deben verificar que la realización de los proyectos de investigación sometidos a su consideración cumplen las normas de BPC.

– Finalmente, es importante resaltar que, tal y como establecen las pautas CIOMS, la utilización de datos identificados para una investigación debería ser excepcional, y que en esos casos los investiga-

dores deberían explicar al comité ético de investigación por qué es necesario mantener los identificativos y cómo se va a proteger la confidencialidad.

5. Criterios que debe aplicar un CEI en la evaluación de proyectos de investigación con tecnología *big data*

En general, la investigación con tecnología *Big Data* utiliza datos anonimizados. Si bien es cierto que, hasta la fecha, la investigación con datos anonimizados había quedado excluida de la legislación y de las pautas éticas sobre investigación biomédica, y por tanto del control ético de los comités, la evolución tecnológica requiere que los estudios con datos anónimos necesiten también un control ético, principalmente por los riesgos asociados a la privacidad. A pesar de no haberse definido explícitamente el tipo de supervisión externa aplicable a estos estudios, la LOPD-GDD parece encomendar su evaluación a los comités de ética de la investigación ya funcionantes en vez de crear nuevos comités expresamente para estos cometidos. En el caso de la utilización de datos seudonimizados o cuando se plantee la reutilización de datos recogidos para finalidades de investigación relacionadas, como se ha comentado previamente, la LOPD-GDD ha introducido la exigencia de evaluación por un comité de ética de la investigación.

Los CEI deben verificar que cualquier proyecto de investigación sometido a su consideración cumple los principios éticos y legales aplicables. En esta línea, en la evaluacion de estudios con *Big Data* debe ponderarse el balance beneficio-riesgo del proyecto, especialmente en relación al riesgo para la intimidad. Por otra parte, teniendo en cuenta el impacto global que pueden tener las tecnologías de análisis de *Big Data* sanitario y las diferentes fuentes de datos disponibles, la revisión ética de estos estudios debería tener en cuenta las diferentes recomendaciones internacionales.

Como reglas generales, los *aspectos que los CEI deberían tener en consideración en la evaluación de proyectos de investigación con tecnología Big Data* son los siguientes:

- El *cumplimiento de los principios éticos* en los que debe sustentarse toda investigación en seres humanos: respeto por las personas, no maleficencia, beneficencia y justicia.

- El valor social y científico de la investigación, sustentado en tres factores: la calidad de la información que ha de producirse, su pertinencia para abordar problemas de salud importantes, y su contribución a la formulación o evaluación de intervenciones, políticas o prácticas que promuevan la salud de las personas o la salud pública.

- La justificación científica y los objetivos del estudio, que deben estar descritos en una memoria científica en la que se refleje la metodología del proyecto, definiendo, entre otros, las variables de resultado, el análisis estadístico previsto o los algoritmos que se vayan a utilizar para analizar los datos. El protocolo o memoria científica debe reflejar cómo se van a tratar los datos obtenidos, los riesgos potenciales para la privacidad y qué medidas se van a adoptar para reducirlos.

  – Se deben exigir documentos que acrediten la idoneidad del investigador. Deberán definirse las funciones y responsabilidades tanto del responsable como del encargado del tratamiento, cuando las funciones de ambos no concurran en la misma persona o institución.

  – Los comités de ética de la investigación, en el procedimiento de evaluación de proyectos de investigación con Big Data en salud, deben verificar el cumplimiento de los aspectos relacionados con el tratamiento de datos de carácter personal y la aplicación del RGPD y la LOPD-GDD[25], comprobando que:

  – Se ha analizado si es necesario realizar una EIPD, tal y como establece el RGPD y la LOPD-GDD y cuando el tratamiento de datos cumpla los criterios de los listados de tratamientos en los que es necesario una EIPD publicados por la AEPD[26], en especial cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales, especialmente si se trata de datos relacionados con la salud, datos genéticos o datos de sujetos vulnerables (discapacitados, menores de 14 años o personas en riesgo de exclusión social).

[25] Apartado 4. Aspectos adicionales que deben revisar los CEI en la evaluación de proyectos de investigación en cumplimiento de las exigencias del RGPD/LOPD-GDD.

[26] Agencia Española de Protección de Datos, *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos* [En línea, consultado 20/09/2019]. Disponible en https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

  - Se van a aplicar medidas técnicas y organizativas para garantizar el respeto del principio de minimización de los datos personales, incluyendo medidas como la anonimización o la seudonimización.

  - Los investigadores han explicitado las políticas de privacidad por diseño y por defecto.

  - El CEI debe comprobar la adecuación de los medios previstos para el tratamiento de los datos, especialmente en lo referente a las medidas de seguridad para garantizar la privacidad, de forma que los datos se almacenen y analicen en servidores seguros. Además debe cumplirse el principio de transparencia, de forma que toda la información pertinente esté a disposición del público.

  - Se debe asegurar la confidencialidad de la información asociada a los datos, compartiendo con los investigadores sólo información codificada o seudonimizada y limitando el acceso a terceros. La identificación de los sujetos debe permanecer en poder del responsable de la custodia de los datos.

  - Los comités deben tener en cuenta que cualquier posible cesión de datos con fines de investigación, además de precisar la obtención del consentimiento expreso de las personas afectadas, deberá realizarse con conocimiento del tipo de datos que se tratarán, el objetivo del tratamiento, durante cuánto tiempo se van a conservar y tratar y si se van a relacionar o cruzar con otros datos procedentes de diferentes fuentes, además de las transferencias previstas a terceros países u organizaciones que no tuviesen un nivel adecuado de protección de datos.

- Deberá analizarse la posibilidad técnica de reidentificación de los sujetos, aspecto especialmente importante si se manejan datos genéticos.

  - En general, los estudios con tecnologías de análisis masivo de datos implican un riesgo mínimo para los sujetos, pero hay circunstancias que pueden aumentar el riesgo, como por ejemplo en temáticas sensibles: maltrato infantil, comportamiento sexual, consumo de drogas ilícitas, o violencia contra la mujer e intrafamiliar; o el riesgo de hacer accesible información privada de los

usuarios de determinados servicios (especialmente si se trata de datos especialmente protegidos). En este sentido, los CEI deben exigir el compromiso escrito del investigador referente a:

– Utilizar los datos sólo para los fines previstos;

– Garantizar la confidencialidad de la información y exigir un compromiso expreso de no realizar ninguna actividad de reidentificación de los participantes ni ceder los datos a terceros no autorizados;

– Cumplir las exigencias legales y del comité respecto al seguimiento, informando periódicamente al CEI sobre la marcha del estudio.

– Garantías de obtención del consentimiento informado en el momento de la recogida de los datos:

– Debe solicitarse el consentimiento expreso de los usuarios para la utilización de los datos de salud con fines diferentes a aquellos para los que se obtuvieron, poniendo en marcha mecanismos eficaces para otorgar o denegar dicho consentimiento. En el caso de datos genéticos el consentimiento debe ser especialmente riguroso dada la posible repercusión para los familiares.

– Cuando se plantee almacenar datos de salud en una base de datos para usos múltiples e indefinidos debe informarse al interesado acerca de estos objetivos. Debe ponerse en conocimiento de los sujetos las medidas de seguridad previstas y los posibles riesgos asociados a la reidentificación y la revelación de información confidencial.

– Los sujetos tienen derecho a recibir la información pertinente en el momento de la recogida de datos, que debe constar, además de los derechos reflejados en el RGPD-LOPD-GDD, al menos de:

– Las reglas de administración de la base de datos;

– El derecho a retirar el consentimiento en cualquier momento y la información identificable de la base de datos de salud, así como

el derecho a solicitar y recibir información sobre sus datos y su uso.

– Es fundamental destacar que el manejo de la ingente cantidad de información en la investigación con tecnología *Big Data* hace impracticable la obtención del consentimiento informado de los sujetos, por lo que podrá aceptarse la realización de este tipo de estudio, sin solicitar el consentimiento informado si se plantea utilizar los datos anonimizados o seudonimizados, con las cautelas previstas en la LOPD-GDD. Esta exención del consentimiento informado puede ser, a su vez, aceptada cuando se plantee reutilizar datos con fines de investigación. En este caso los CEI deberán verificar las exigencias de la LOPD-GDD, comprobando que la información esté disponible en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación. Esta información debe describir, al menos, la identidad y datos de contacto del responsable del tratamiento, los fines del tratamiento, los destinatarios de los datos o la posibilidad de transferencia de datos personales a terceros países.

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

– Tal y como establece la legislación aplicable y según recomiendan las pautas CIOMS, los CEI, cuando acepten la exención de consentimiento informado, deberían verificar que se cumplan las siguientes premisas:

- Se cumplen las condiciones legalmente establecidas para la exención del consentimiento si se utilizan datos seudonimizados o anonimizados;

- En los supuestos de reutilización de datos con fines de investigación se informe adecuadamente a los sujetos, a través de la página web de la institución, informando sobre el derecho de revocación y notificar la existencia de esta información por medios electrónicos a los afectados.

- La investigación implique un riesgo mínimo para los sujetos;
- La investigación tiene un valor social importante
- No tenga implicaciones en los derechos y bienestar de los sujetos;
- La investigación no pueda llevarse a cabo sin la exención del consentimiento;
  - Tal y como exige la LOPD-GDD y establecen las pautas CIOMS, el investigador debería obtener un consentimiento informado explícito para utilizar los datos relacionados con la salud para investigación biomédica, salvo en los casos que cumplan los requisitos establecidos por la LOPD-GDD para la exención del consentimiento, especialmente si se cumplen las siguientes circunstancias: si la investigación implica riesgos superiores al mínimo para el sujeto; cuando se utilicen técnicas controvertidas o de alto impacto, aunque estén aprobadas, y cuando la investigación se desarrolle en entornos de alta vulnerabilidad, exigiendo en estos casos una EIPD como garantía adicional.
  - El RGPD y la LOPD-GDD hacen referencia al derecho de retirar el consentimiento en cualquier momento, sin que ello afecte a los tratamientos efectuados previos a esta retirada. En esta línea los CEI deberían comprobar: que el titular de los datos sea consciente de su existencia; que se proporcione información suficiente y que se informe sobre el derecho a solicitar la cancelacion de los datos.
  - Los CEI deben colaborar en difundir las exigencias del nuevo marco normativo, asesorando en la elaboración de consentimientos amplios, que podrían ser válidos para áreas de investigación relacionadas con la misma especialidad médica o investigadora. Estos consentimiento facilitarán la realizacion de estudios con *Big Data*. A su vez, se debería consultar con las autoridades de control la opción de solicitar consentimientos amplios para asistencia e investigación, de forma que el interesado o, en su caso, su representante legal pudiera otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, biomédica. Estos modelos de consentimiento deberían ser aprobados por los CEI.

6. Adaptación de los CEI a la evaluación de proyectos con tecnología *big data*

Los comités de ética de la investigación, en el procedimiento de evaluación de estudios, deben llevar a cabo una deliberación ética, teniendo en cuenta los principios y valores de la ética de la investigación incluidos en las directrices internacionales. Las decisiones serán válidas siempre y cuando sean el resultado de deliberaciones honestas, justas y bien informadas. En base a esta premisa, para evaluar los proyectos de investigación con tecnología *Big Data*, los CEI deben adaptarse, tanto en composición como en funcionamiento, a las exigencias requeridas tanto por la normativa como por la tecnología a utilizar.

En relación a la *adecuación en la composición*, los CEI deberían contar con bioinformáticos o con otros expertos en este tipo de tecnología y en las medidas de seguridad asociadas. Si no se dispusiera de esta opción, cuando se remitieran para su consideración proyectos de investigación con tecnología *Big Data*, podría solicitarse el asesoramiento de expertos independientes, en analogía a lo exigido en el Real Decreto 1090/2015, en relación a la evaluación de estudios con procedimientos quirúrgicos, técnicas diagnósticas, productos sanitarios o terapias avanzadas. En este caso, sería conveniente que los CEI contaran con un listado de expertos que firmaran los correspondientes compromisos de confidencialidad y de ausencia de conflicto de interés, al igual que los miembros acreditados del comité.

Por otra parte, en la evaluación de este tipo de estudios, los CEI deben garantizar el *cumplimiento de lo establecido en el nuevo marco normativo* (RGPD/LOPD-GDD). En este sentido, tal y como se ha descrito previamente, la LOPD-GDD ha establecido que, en el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados. En esta línea, hay que recordar que la LOPD-GDD exige que los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes cuenten con un delegado de protección de datos. Por otra parte, deberán definirse los criterios para el nombramiento de un experto con los conocimientos suficientes del Reglamento (UE) 2016/679.

Es imperativo que las personas que forman parte de los comités reciban *formación* en las nuevas exigencias del marco normativo, así como en las innovaciones tecnológicas. Además, para que el CEI pueda asumir estas nuevas funciones es imprescindible la *coordinación con las autoridades de control y con los DPD* de los centros investigadores, que deben implementar las directrices para que los investigadores puedan realizar los proyectos conforme a la normativa de protección de datos.

Para adaptarse a los nuevos requerimientos del RGPD y las particularidades de la tecnología *Big Data*, los CEI deberían establecer *requisitos de evaluación específicos* y *adecuar los procedimientos normalizados de trabajo*, de forma que recojan las exigencias, tanto de la nueva normativa como de los avances tecnológicos. En este sentido, en el procedimiento de evaluación de estudios con *Big Data* deberían incluirse protocolos de evaluación del riesgo de la tecnología. Estos documentos deberían estar públicamente accesibles, para facilitar la tramitación de la solicitud de evaluación de proyectos de investigación por parte de los investigadores.

Hay que tener en cuenta que, hasta la fecha, no existía la exigencia legal de que los estudios observacionales con datos personales fueran evaluados por un CEI; de esta manera, con la entrada en vigor de la nueva Ley, se prevé un aumento de la carga de trabajo de los comités.

7. Seguimiento de la investigación de estudios *big data* por los comités

Los CEI tienen la obligación legal de realizar el seguimiento de los estudios que han aprobado[27]. Algunas de las actividades que los CEI pueden realizar para llevar a cabo este seguimiento son:

– Verificar que se cumplen las condiciones de realización de los estudios, tanto respecto a los términos en los que se otorgó el consentimiento, si fue solicitado, como respecto a la nueva información relevante disponible que pudiera ser de interés para el estudio y/o que pudiera ser incorporada a la información a suministrar a los sujetos.

[27] Artículo 25. Comprobaciones sobre el curso de la investigación. Ley 14/2007, de 3 de julio, de investigación biomédica.

– Asegurar que los titulares de los datos pueden acceder a la información relevante obtenida en el estudio. Además, deben verificar que la información sobre los estudios en los que se reutilizan datos de investigaciones previas está publicada en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor.

– Realizar un seguimiento sobre la seguridad del tratamiento de los datos personales, especialmente si se externalizan las actividades relacionadas con su explotación.

– Comprobar la publicación de los resultados, una vez finalizados los estudios.

Para dar cumplimiento a estas funciones, el CEI debe monitorizar la marcha del estudio mediante la solicitud de información periódica, o incluso mediante la verificación de las condiciones de realización de los estudios en marcha, a traves de visitas de comprobación al centro investigador. A su vez, el investigador tendrá que informar regularmente al CEI de la situación del estudio.

8. Conclusiones

La utilización de la tecnología *Big Data* en asistencia sanitaria ha supuesto un cambio sustancial en el manejo y control de las enfermedades, especialmente en aquellas de curso crónico. A su vez, la investigación con esta tecnología permite un análisis más rápido, exacto y eficiente de la información clínica, al procesar grandes cantidades de datos de diferentes pacientes, facilitando el acceso a nuevos conocimientos y su posterior diseminación.

La investigación con tecnología *Big Data* en el ámbito sanitario debe contar con un procedimiento adecuado, transparente y seguro, en el contexto de un marco ético y jurídico que garantice el máximo nivel de protección en el tratamiento de datos de carácter personal.

La tecnología *Big Data* maneja en general datos anonimizados. La anonimización representaba hasta hace poco tiempo la garantía de cumplimiento de la regulación de protección de datos personales, partiendo de que los datos anonimizados dejaban de ser datos personales, no precisando protección legal. No obstante, actualmente la anonimización no garantiza

la privacidad de los datos personales, puesto que mediante técnicas de ingeniería informática podría ser posible volver a conectar los datos con la persona a quien pertenecen, permitiendo la desanonimización, reidentificación, o revelación de datos personales de conjuntos de usuarios y de usuarios individuales. Por este motivo, el riesgo principal de los estudios con *Big Data* radica en la potencial amenaza para la privacidad de los sujetos de quienes proceden los datos.

A pesar de que la legislación vigente o incluso las referencias éticas internacionales, como la Declaración de Helsinki, no hacen referencia explícita al control ético de los proyectos de investigación realizados con datos anónimos o anonimizados, teniendo en cuenta los riesgos para la privacidad de la personas de las que proceden los datos, es esencial proteger sus derechos mediante una revisión ética de los proyectos de investigación con tecnologías *Big Data*. Esta evaluación debe ser realizada por los comités de ética de la investigación, ponderando tanto los posibles beneficios para la sociedad como los riesgos teóricos para los sujetos.

La realización de estudios con *Big Data* debe cumplir las exigencias de la nueva legislación de protección de datos (RGPD y LOPD-GDD), que han adoptado un enfoque preventivo en cuanto a los principios de la protección de datos desde el diseño y por defecto, que deben aplicarse siempre que sea posible para el desarrollo de la investigación. Por otra parte, la nueva legislación ha introducido un nuevo tratamiento de datos, la seudonimización, como herramienta válida para garantizar la privacidad de los datos personales, permitiendo el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica, siempre y cuando se cumplan unos requisitos de seguridad adicionales.

La LOPD-GDD atribuye a los CEI la responsabilidad de establecer el control ético de la investigación con datos personales. Si bien es cierto que exige, de forma explícita, el informe del CEI cuando se plantee utilizar con fines de investigación datos seudonimizados, o cuando vayan a reutilizarse datos personales recogidos después de la entrada en vigor de la LOPD-GDD, es importante resaltar el papel que asigna a los CEI en la investigacion con otras categorías de datos. Así, establece las exigencias de composición del CEI (DPD o experto en el RGPD) cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Los comités de ética de la investigación, como garantes de los derechos, seguridad y bienestar de los sujetos que participan en un proyecto de investigación biomédica, deben verificar la pertinencia del estudio, su diseño metodológico y las medidas para garantizar la confidencialidad y la seguridad de los datos. A su vez, deben comprobar el respeto a los derechos de los titulares de los datos y el cumplimiento de los principios éticos que deben guiar el tratamiento de los datos, de forma que no vayan a ser recogidos ni tratados para cualquier uso, sino solo para unos objetivos específicos y legítimos que hayan sido prefijados. En base a la aplicación del RGPD y de la nueva LOPD, los CEI deberán comprobar que los estudios que evalúan disponen de planes de protección de datos. Además, deben revisar las condiciones de obtención del consentimiento informado, incluyendo las posibles exenciones.

Los CEI deben adaptar los procedimientos normalizados de trabajo para asumir con plenas garantías las nuevas exigencias, introducidas tanto por el RGPD/LOPD-GDD como por el uso de la tecnología en el tratamiento de los datos. Por otra parte, deben desempeñar un papel clave en el seguimiento de los proyectos, verificando que su realización ha sido acorde a los principios éticos y a la legislación vigente y que toda la información pertinente está a disposición del público.

Los CEI deben colaborar en difundir las exigencias del nuevo marco normativo, asesorando en la elaboración de consentimientos amplios, que podrían ser válidos para áreas de investigación relacionadas con la misma especialidad médica o investigadora. Estos consentimiento facilitarán la realizacion de estudios con *Big Data*.

Es necesario resaltar que la referencia a la investigación con datos de salud en una disposición adicional y en una disposición transitoria no ha clarificado ni los requisitos ni el procedimiento de evaluación de estos estudios. Así, algunos aspectos cruciales no han sido resueltos, como las garantías de los titulares de los datos obtenidos antes de la publicación de la LOPD-GDD cuando se plantea su posterior reutilización con fines de investigación. Por ello, el legislador debería plantear la modificación de la legislación vigente, clarificando la función de los comités de ética de la investigación, tanto en la evaluación de los proyectos con datos de salud en general, como de forma específica en los estudios con tecnología *Big Data*.

Finalmente, los CEI deberían desempeñar un papel proactivo en la difusión de los principios éticos y legales, de cara a fomentar una cultura de respeto por la intimidad y la confidencialidad de los datos personales,

tanto en la comunidad científica como en la sociedad en general. Los CEI deben contribuir al debate social sobre estas cuestiones, promoviendo una cultura de la privacidad; además, deben desarrollar su capacidad formativa y sensibilizadora en cuestiones tan relevantes como la protección de los datos de las personas en investigación en salud, especialmente cuando puedan afectar a población vulnerable.

Protección de los datos personales de salud en el proceso penal: efectos en la valoración de la prueba*

Protection of personal health data in criminal proceedings: effects on the evaluation of evidence

Profa. Dra. Miren Josune Pérez Estrada

Prof. Adjunta (Acred. Agregada) de Derecho Procesal, Universidad del País Vasco UPV/EHU (Bilbao, España)

DOI: 10.14679/1142

Sumario / Summary: 1. Planteamiento. 2. La limitación del derecho fundamental a la protección de los datos personales en el proceso penal. 3. La protección de los datos personales de salud en el proceso penal. 3.1. Régimen jurídico de los datos personales de salud contenidos en los informes clínicos. 3.2. Tratamiento procesal de los datos personales de salud. 4. Protección de los datos personales frente a los nuevos métodos de investigación tecnológica en el proceso penal. 4.1. Regulación de las medidas de investigación tecnológica. 4.2. Los dispositivos de almacenamiento masivo de información. 4.3. Ilicitud de la prueba tecnológica obtenida vulnerando el derecho fundamental a la protección de los datos de carácter personal.

Resumen / Abstract: Este trabajo cuestiona el valor que se debe dar a la prueba que se ha obtenido vulnerando el derecho fundamental a la protección de los datos personales, en general, y a los relativos a la salud, en particular y cuáles deben ser las consecuencias de esa valoración judicial en el proceso penal. Se reclama una regulación procesal más precisa que otorgue mayores garantías al tratamiento de los datos personales del investigado en el proceso penal con el fin de evitar la vulneración de este derecho.

This research paper questions the value that should be given to the evidence that has been obtained in violation of the fundamental right to the protection of

* Artículo recibido el 18 de febrero de 2019 y aceptado para su publicación el 30 de mayo de 2019.

personal data, in general, and those relating to health, in particular, and what the consequences of that should be judicial evaluation in the criminal process. It demands a more precise procedural regulation that grants greater guarantees to the treatment of the personal data of the investigated in the criminal process in order to avoid the violation of this right

Palabras clave / Keywords:

Prueba ilícita / Protección de datos de carácter personal / Datos relativos a la salud / Entorno virtual / Garantías procesales.

Unlawful proof / Protection of personal data / Data related to health / Virtual environment / Procedural guarantees.

1. Planteamiento

En el proceso penal los datos médicos que se incorporan a las actuaciones están relacionados con la actividad probatoria: constituyen una fuente de prueba o hacen prueba en sí mismos. La incorporación al proceso penal de este tipo de datos a través de la prueba documental y de la prueba pericial médica hace que nos encontraremos en el proceso penal con dos tipos de aportaciones de datos médicos: los procedentes de informes clínicos y aquellos contenidos en los informes médico-periciales.

La existencia de estos datos sensibles, como son los de la salud, en el proceso penal contenidos en los informes médicos unida a la digitalización de la justicia[1] permite el tratamiento de gran cantidad de este tipo de datos personales; si bien, la finalidad de su tratamiento está encaminado a que sirvan de prueba en el proceso penal.

La comisión de un delito justifica el acceso a los datos personales, también a los de salud, del investigado. Esta intromisión en los datos personales que, en principio, aparece justificada en la comisión del delito precisa de matizaciones. Estas matizaciones deben provenir de la gravedad del delito cometido y de la gravedad de la injerencia, a través de sus datos personales, en la vida privada del individuo investigado. A través de este trabajo se cuestiona el valor que se debe dar a la prueba que se ha obtenido vulnerando

[1] La digitalización de la justicia es fruto de una aspiración mayor cual es la modernización de la justicia en la que uno de sus pilares lo ha constituido la informatización como soporte de programas de gestión procesal superada hoy por un "entramado de aplicaciones de gestión, de obtención de datos y de comunicaciones" manejadas a través de la intranet accediendo al "Punto Neutro Judicial" (PNJ), que administra el Consejo General del Poder Judicial. Cabezudo Rodríguez, Nicolás, "Datos personales e informaciones judiciales", *Revista General de Derecho procesal*, Núm. 17, 2009, estudia los diferentes ficheros de datos de carácter personal de la Administración de Justicia.

el derecho fundamental a la protección de los datos personales, en general, y de los relativos a la salud, en particular y cuáles son las consecuencias de esa valoración en el proceso penal. También se reclama una regulación procesal específica que otorgue mayores garantías al tratamiento de los datos personales del investigado en el proceso con el fin de evitar la vulneración de este derecho.

2. La limitación del derecho fundamental a la protección de los datos personales en el proceso penal

El derecho fundamental a la protección de los datos que se contiene en el art. 18.4 CE[2] no es absoluto. La limitación de su ejercicio viene dada de forma genérica por el propia Constitución, en el art. 10.1, cuando se residencia en el orden público y la paz social[3] y por el TC cuando limita el derecho fundamental a la protección de los datos personales por, entre otros, la averiguación, persecución y castigo del delito[4]. Además, el resto de derechos fundamentales y bienes jurídicos protegidos constitucionalmente actúan también como límite al ejercicio del derecho fundamental a la protección de los datos personales, en atención a la necesidad, proporcionalidad y a que el fin legítimo que se persigue sea "respetuoso con el contenido esencial del derecho fundamental restringido"[5].

---

[2] La protección de los datos personales no se recoge expresamente en el art. 18.4 CE pero sí se contiene en él como protección contra las amenazas a la dignidad, identidad, libertad e intimidad de las personas. Estamos ante un derecho que pone de manifiesto la necesaria protección de los datos personales frente al tratamiento automatizado de los mismos que afecta al control de "nuestras vidas y personalidad" .

[3] Art. 10.1 CE: "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".

[4] Lo recuerda la STC 292/2000, en su FJ 9: "En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (por citar las más recientes, SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio)".

[5] De esta manera lo recoge el FJ 11 de la STC 292/2000 : "…este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos

Además del límite anterior, que podríamos englobarlo en una categoría general, existe uno específico, propio del desarrollo del proceso penal. Así, el derecho a la protección de los datos personales encontrará límites específicos entre los derechos que protege el art. 24 CE[6] y que afecta al tratamiento de los datos personales del investigado en el proceso. Se trata de la tutela judicial efectiva, el derecho a un proceso con todas las garantías, derecho de defensa y el derecho a la prueba. Por lo tanto, debemos entender que el derecho a la protección de los datos personales del investigado o encausado, *i.e.*, el poder de control, de disposición de sus datos personales que se traduce en la imposición a terceros de determinados deberes de hacer: "el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos" cede o "presenta ciertas limitaciones" en el transcurso del proceso penal con el fin de conseguir llevar a buen término la investigación penal[7].

---

constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5). (…) Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2)".

[6] Art. 24 CE: 1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión.
2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

[7] STC 254/1993, de 20 de julio, FJ 7. De esta manera el autor Marcos Ayjón, Miguel, "Las múltiples implicaciones de la protección de datos en la justicia penal", *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario ReDPE*, AAVV (coord. Gutiérrez Zarza, María Ángeles), 2018, p. 15, considera una posible colisión de derechos procesales constitucionalizados: derecho a la tutela judicial efectiva y ejercicio de defensa (art. 24 CE), libertad de información (art. 20 CE) y publicidad de las actuaciones (art. 120.1 CE). "Estos tres derechos son difíciles de conciliar con el derecho a la protección de datos, puesto que, a más información y acceso, menor protección de los datos personales contenidos en el mismo. La frecuente colisión entre ellos deberá resolverse de acuerdo con lo dispuesto en las normas procesales aplicables al efecto y siempre bajo los criterios de proporcionalidad. Ahora bien, eso no impide establecer como principio general que, en el supuesto de colisionar la tutela judicial y el derecho de defensa con la protección de los datos personales, prevalece el derecho fundamental de defensa, sin perjuicio de que deba intentarse la cohabitación entre ambos".

El asunto radica en la normativa que se debe aplicar en el caso de colisión de estos derechos del art. 24 CE con el de la protección de datos personales. Es decir, si para solucionarlo se aplica la regulación general sobre protección de datos o si, por el contrario, habrá de estarse a la norma procesal. El legislador parece dudar: el art. 236 bis LOPJ establece que el tratamiento de los datos personales que se realice por los tribunales se debe someter a la normativa sustantiva común de protección de datos personales pero el siguiente artículo, 236 *quáter* LOPJ exime a los tribunales de que el interesado preste su consentimiento para el tratamiento de los datos personales en el ejercicio de la potestad jurisdiccional y dispone que será necesario someterse a las normas procesales sobre la validez de la prueba. El tratamiento de los datos de carácter personal que se lleva a cabo en el ámbito jurisdiccional debería regularse por normativa procesal cediendo, en este caso, la general de protección de datos personales. En un futuro la norma procesal deberá desarrollarse con mayor amplitud para dar mayor y mejor cobertura legal a la protección de los datos personales del investigado o encausado en el proceso penal.

3. La protección de los datos personales de salud en el proceso penal

3.1. Régimen jurídico de los datos personales de salud contenidos en los informes clínicos

La regulación de los informes clínicos que contienen los datos especialmente protegidos como son los referentes a la salud[8], ha sido objeto de atención por parte del legislador a través de diferentes instrumentos jurídicos[9], La ley 41/2002, de 14 de noviembre, básica reguladora de la auto-

[8] Se consideran datos de carácter personal relacionados con la salud "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas, los referidos a sus porcentajes de discapacidad y a su información genética", art. 5.1 g) del Reglamento de la LOPD.

[9] Se trata de una regulación dispersa, problema que expone la propia exposición de Motivos del RD 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud., en su párrafo 7: "Este real decreto, atendidas la diversidad de sistemas y tipos de historias clínicas vigentes en el ámbito de cada comunidad autónoma, y con el consenso de profesionales sanitarios de distintas áreas de conocimiento, pretende establecer el conjunto mínimo de datos que deberán contener una serie de documentos clínicos con el fin de compatibilizar y hacer posible su uso por todos los centros y dispositivos asistenciales que integran el Sistema Nacional de Salud".

nomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[10] y el RD 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud[11].

El art. 3 de la Ley 41/2002 diferencia entre los conceptos "historia clínica" e "información clínica"; así, "historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial" e "información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla". [12] Si bien la finalidad de ambos es su uso en el ámbito asistencial, como se establece en el art. 15 en relación con el art. 16 de la Ley 41/2202, también permiten incorporar a las actuaciones judiciales datos personales relativos a la salud. Dispone el art. 15. 2 de la Ley 41/2202: "La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud". Y el art. 16.1 de la Ley 41/2002: "La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente". El mismo artículo en el punto 3: "El acceso a la historia clínica con fines judiciales…se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales…"[13].

---

[10] BOE núm. 274, de 15/11/2002. Como antecedente a la regulación nacional de la documentación clínica encontramos el Convenio del Consejo de Europa sobre derechos humanos y biomedicina, de 4 de abril de 1997, ratificado por España, 23 de julio de 1999.

[11] BOE núm. 225, de 16 de septiembre de 2010.

[12] Flores Prada, Ignacio, "Algunas consideraciones sobre el régimen jurídico-procesal de los informes clínicos", *Revista Electrónica de Ciencia Penal y Criminología"*, Núm. 15-17, 2013, pp. 6-7 considera que la definición que otorga la ley sobre información clínica puede acarrear discusión entre lo que debe considerarse como informe clínico y lo que es informe pericial. De esta manera, considera que "… la categoría no es el informe clínico sino el informe médico, y que dentro de dicha categoría pueden distinguirse como especies, a los efectos que en este trabajo interesan, los documentos propiamente médicos, y los documentos médico-legales. Los informes clínicos pertenecen a la especie de documentos propiamente médicos, mientras que los informes periciales constituyen informes médico-legales. Puede hablarse así de informes médico-clínicos e informes médico-periciales". Sobre este tema Romeo Casabona, Carlos María / Castellano Arroyo, "La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica", *Derecho y Salud*, Núm. 1, 1993, pp. 4-19.

[13] El precepto en su totalidad es el que sigue: "El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en

Una de las cuestiones que mayor dedicación ocupa es la de concretar qué datos de salud son necesarios incorporar al proceso. Habrá que ponderar en cada caso los datos de interés para el proceso valorando la situación con el fin de evitar conculcar el derecho de defensa, así como lograr que se respete el principio de contradicción que rige entre las partes. Para lograr este cometido es necesario tener en cuenta el RD 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud[14]. Como se recoge en la Exposición de Motivos del RD 1093/2010 una de las tareas que se contienen es la de definir el conjunto de datos que, por su relevancia, deben estar contenidos en los diferentes informes clínicos. Esta sistematización del contenido mínimo que debe contener la información clínica facilitará la labor de los tribunales sobre la petición e incorporación de sólo los datos de salud útiles al proceso o acordes con su objeto, evitando así la práctica de incorporar al proceso la información clínica completa[15].

3.2. Tratamiento procesal de los datos personales de salud

La importancia de los datos personales relativos a la salud en el ámbito procesal la encontramos en el hecho de que la documentación médica que contiene ese tipo de datos es una fuente de prueba para el proceso. Se trata de una prueba de naturaleza documental[16] que se trae al proceso con la finalidad de acreditar determinados hechos médicos. Este tipo de prueba se regula, de manera general, en la Ley de Enjuiciamiento Civil (LEC), arts. 264 a 272 y 324 a 334[17], con directa aplicación en el proceso civil pero que actúa de manera subsidiaria para el resto de procesos.

Son numerosos los datos relativos a la salud que se pueden incorporar al proceso y pueden llegar a través de distintos documentos. Podría ser útil

---

la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso".

[14] BOE núm. 225, de 16 de septiembre de 2010.

[15] En palabras de Flores Prada, Ignacio, "Algunas consideraciones sobre el régimen jurídico-procesal de los informes clínicos", *Revista Electrónica de Ciencia Penal y Criminología*, *op. cit.* p. 10, "Todo ello contribuirá a evitar la perniciosa práctica de solicitar (por elevación) la información clínica completa, manteniéndose en límites razonables y proporcionales la intimidad del paciente y la reserva sobre otros datos de la historia clínica no relevantes para el proceso en cuestión".

[16] Son numerosas las ocasiones en las que el TS se ha pronunciado sobre el carácter documental de la historia clínica, entre otras, STS 878/1994, de 5 de junio de 1998, STS 2249/1999, de 14 de febrero de 2006, y STS 5938/2011, de 27 de noviembre de 2012.

[17] Hacen referencia a la forma de presentación de documentos, dictámenes, informes y otros medios e instrumentos y a los documentos privados, respectivamente.

establecer una clasificación que diferencie entre informes médicos e informes médico-legales; dentro de los primeros encontraríamos los informes clínicos y en los segundos estarían los informes médico-periciales. La distinción es importante por tener ambos documentos un diferente régimen procesal. Los primeros, considerados como fuente de prueba documental, servirán para acreditar los datos que se encuentran relacionados con el tratamiento asistencial o sanitario recibido y los informes médico-legales servirán para acreditar hechos médicos diferentes de los contenidos en el tratamiento asistencial, con la finalidad de certificar datos médicos alegados por la parte interesada[18].

La aportación al proceso penal de los datos relativos la salud[19] se produce, o bien de oficio o a instancia de parte. En el caso de la petición de oficio[20] la misma viene avalada por el art. 16 de la Ley 41/2002, que prevé

[18] Esta distinción entre ambos documentos la desarrolla Flores Prada, Ignacio, "Algunas consideraciones sobre el régimen jurídico-procesal de los informes clínicos", *Revista Electrónica de Ciencia Penal y Criminología*, *op. cit*. pp. 12-13. Señala el autor que la diferencia entre informe clínico e informe pericial se mueve en tres ámbitos: autoría, contenido y finalidad: "…el informe clínico es elaborado por el médico o personal sanitario que trata al paciente. El perito médico tiene con el paciente una relación no terapéutica sino analítica. El perito surge en el proceso y por causa del proceso…" Como efecto señala que "el autor del informe clínico pueda comparecer en el proceso, a lo más, como testigo-perito, pero nunca como perito stricto sensu". Teniendo en cuenta el contenido del informe, "…el documento clínico contiene datos, opiniones, resultados, diagnósticos, pronósticos o evaluaciones vinculadas con la salud del paciente. Refleja, pues, contenidos terapéuticos, análisis de estrategias o informaciones clínicas surgidas en el curso del tratamiento médico. Por el contrario, el informe pericial contiene máximas de experiencia, abstractas o aplicadas, que tratan de relacionar el estado de salud del sujeto con determinados hechos o circunstancias, que generalmente tienen la consideración de "efectos" de la salud del sujeto sobre ciertos aspectos de la realidad con trascendencia jurídica. Tomando en consideración su finalidad, el informe clínico persigue contribuir al tratamiento y curación del sujeto, mientras que el informe pericial cumple únicamente una función analítica e informativa externa de la salud del sujeto en conexión con determinadas parcelas de su conducta".

[19] Podemos ver al respecto, Gómez Álvarez, Francisco Javier, "La cesión de datos de carácter personal al proceso penal, en especial los datos relativos a la salud", *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, AAVV (coord. Oubiña Barbolla, Sabela / Catalina Benavente, María Ángeles (Dir. Colomer Hernández, Ignacio), 2017, pp. 607-646.

[20] La aportación de la información clínica constituye una obligación de carácter general de las administración y ciudadanos de colaboración con la autoridad judicial que se impone en el art. 118 CE: "Es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto".

el acceso judicial a la información clínica[21], con remisión a la legislación general de protección de los datos[22]. Cuestión importante en este tema es la incorporación a las actuaciones judiciales de datos relativos a la salud que provienen de la documentación incautada o almacenada en dispositivos electrónicos en realización de la diligencia de investigación de registro[23], cuya problemática trataremos en epígrafe posterior pero que ya adelantamos que no deben de aprehenderse más datos relativos a la salud que los autorizados judicialmente.

Sobre la aportación de parte[24], en el supuesto de admitirse prueba pericial privada, el órgano jurisdiccional deberá valorar la necesidad del acceso a datos relativos a la salud de la parte que sean necesarios para la realización del examen y si su negativa puede vulnerar el derecho de defensa. Pues se puede dar el supuesto que el juez acuerde la admisión de la prueba pericial, pero deniegue la petición de acceso a datos relativos a la salud contenidos en informes médicos que sean necesarios para la elaboración del informe pericial. Esta situación podría suponer la vulneración del derecho fundamental

[21] El punto 3 del art. 16 de la Ley 41/2002 establece: "El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Asimismo, se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".

[22] Sin necesidad de que el titular de los datos preste su consentimiento para la cesión de los mismos al tratarse de un requerimiento judicial en cumplimiento de las funciones encomendadas, de acuerdo con el art. 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[23] Para la que será necesario, salvo supuestos de urgencia, que la policía cuente con autorización judicial como así lo pone de relieve Troncoso Reigada, Antonio, *La protección de datos personales en busca de equilibrio*, Ed. Tirant lo Blanch, Valencia, España, 2010, p. 53, *i.e.,* que "utilice el mismo procedimiento para el acceso a datos de salud que para la entrada en domicilio o la interceptación de las comunicaciones…"

[24] Por el autor Flores Prada Ignacio, "Algunas consideraciones sobre el régimen jurídico-procesal de los informes clínicos", *Revista Electrónica de Ciencia Penal y Criminología*, *op. cit*. pp. 20-25, se recogen los supuestos de aportación de parte al proceso de datos relativos a la salud, teniendo en cuenta tanto el proceso penal como el proceso civil.

de defensa recogido en el art. 24.1 CE[25]. Una posible solución a esta cuestión la podríamos encontrar en la posibilidad de que el juez acordar ciertos límites en el acceso a los datos de salud teniendo en cuenta sólo la utilización de los que sean necesarios para la realización del informe y sin necesidad de tener que aportar todos los datos de salud a la causa[26].

4. Protección de los datos personales frente a los métodos de investigación tecnológica en el proceso penal

4.1. Regulación de las medidas de investigación tecnológica

Sobre la situación actual de la regulación de las medidas de investigación tecnológica en el proceso penal la reforma de la Ley de Enjuiciamiento Criminal (LECr) por la LO 13/2015, de 5 de octubre, de modificación de la LECr para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[27], supuso dar cobertura legal a las diligencias de investigación tecnológica[28]. De esta manera, se regulan las diligencias de investigación de intervención de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Se trata de los Capítulos IV a X del Título VIII ("De las medidas

[25] Sentencia del Tribunal Supremo 3475/2000, de 25 de abril de 2000, F.J. 5ª: "… la historia clínica completa del recurrente era sin duda pertinente, dado que tiene referencias a aspectos, tales como las curas de desintoxicación y duración de la adicción, que son relevantes para establecer los presupuestos de la eventual aplicación del art. 21.1 y 2 CP. Como es sabido la jurisprudencia de esta Sala otorga significación, a los efectos de establecer la capacidad de culpabilidad o su disminución, a la larga duración de la dependencia de drogas que causan grave daño a la salud.
Consecuentemente, el recurrente ha sido privado del derecho a valerse de pruebas pertinentes que le garantiza el art. 24.2 CE y por tal razón la sentencia incurre en el quebrantamiento de forma que prevé el art. 850.1 LECr"..

[26] En los casos del requerimiento judicial es necesario que la petición judicial esté motivada y concrete los documentos de la historia clínica que son necesarios conocer para la investigación de los hechos. Se trata de aportar al proceso la documentación necesaria evitando aportación de datos relativos a la salud innecesarios para el proceso. Así lo señala Sarrato Martínez, Luis, "La historia clínica y su acceso con fines judiciales", *Diario La Ley*, Núm. 6854, 2008.

[27] BOE núm. 239, de 6/10/2015.

[28] Anteriormente, no existía una regulación concreta de esta materia en la LECr. En los supuestos de acceso a la prueba electrónica se aplicaban por analogía preceptos de la LECr y la amplía doctrina jurisprudencial que sí se había desarrollado en esta materia.

de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"), art. 588 bis a 588 octies.

La nueva regulación pretendió dotar de mayor eficacia al derecho procesal a la vez que procuraba se actuase con pleno respeto a las garantías del proceso cuando se vieran afectados derechos fundamentales de la persona, reconocidos en el art. 18 LECr[29]. Y es que la regulación de estas diligencias de investigación había sido ampliamente demandada por la doctrina[30] y jurisprudencia; en ese sentido, por todas, la STC 145/2014 recordaba la necesidad de una habilitación legal en los supuestos de injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas.

Con la reforma de la LECr se cumple con las obligaciones que resultan de la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001[31], que se aplica a la obtención de pruebas electrónicas[32] y se ha dado cobertura legal a las medidas de investigación tecnológica, siguiendo la jurisprudencia de la Sala de lo Penal del TS. Así, destacamos entre la numerosa doctrina jurisprudencial las siguientes sentencias del TS: STS 250/2017, de 5 de abril[33], sienta la doctrina general sobre los presupuestos necesarios para la autorización de la interceptación de las comunicaciones

---

29 Véase la Exposición de Motivos, apartado IV.

30 Sobre este tema, véase, entre otros, Etxeberria Guridi, José Francisco, *La protección de los datos de carácter personal en el ámbito de la investigación penal*, Agencia de protección de Datos, Premio Protección de datos Personales, Madrid, España, 1998, p. 22, Castillejo Manzanares, Raquel, *Hacia un nuevo proceso penal*, La Ley, Madrid, España, 2010 y Banacloche Palao, Julio / Zarzalejos Nieto, Jesús, "Las diligencias de investigación restrictivas de los derechos fundamentales", *Aspectos fundamentales del Derecho Procesal Penal"*, *La Ley*, Madrid, España, 3ª ed., 2015.

31 BOE núm. 226, de 17 de septiembre de 2010.

32 Art. 14.2 c) Convenio de Budapest sobre Ciberdelincuencia. La prueba electrónica o en soporte electrónico la define Sanchís Crespo, Carolina, "La prueba en soporte electrónico", *Las tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio,* AAVV (coords. Gamero Casado, Eduardo / Valero Torrijos, Julián), Thomson Reuters-Aranzadi, Navarra, España, 2012, p. 713, como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal". Con carácter general, la prueba en el proceso penal cabe definirla como "la actividad procesal, de las partes (de demostración) y del juez (de verificación), por la que se pretende lograr el convencimiento psicológico del juzgador acerca de la verdad de los datos alegados al proceso". De esta manera, la describe Barona Vilar, Silvia, "La prueba (I)", AA.VV. (Montero Aroca, Juan / Gómez Colomer, Juan Luis / Barona vilar, Silvia / Esparza Leibar, Iñaki / Etxebarria Guridi, José Francisco), *Derecho Jurisdiccional III. Proceso Penal,* 25ª ed., Ed. Tirant lo Blanch, Valencia, España, 2018, p. 38.

33 Roj: STS 1582/2017 - ECLI: ES:TS:2017:1582.

telefónicas y telemáticas, STS 272/2017, de 18 de abril[34], sobre la utilización de dispositivos técnicos de captación de la imagen con motivo de la nueva regulación de la LECr y STS 786/2015, de 4 de diciembre[35], sobre registro de dispositivos de almacenamiento masivo de información, en este caso acceso al contenido de ordenadores; importa resaltar en esta sentencia la doctrina jurisprudencial sobre el derecho al propio entorno virtual[36].

La utilización habitual de las nuevas tecnologías hace necesaria la obtención de prueba de tipo tecnológico que, si bien es cierto, que contribuirá a incrementar la eficacia judicial en la persecución de los delitos, en igual medida aumentará el riesgo de lesividad del derecho fundamental a la protección de los datos personales de las personas investigadas. A pesar de ello, no se ha aprovechado la reforma de la legislación procesal para haber realizado una protección específica del derecho a la protección de los datos personales que pudiera verse afectado con motivo de la obtención de prueba tecnológica. Del elenco de medidas de investigación tecnológica que se regulan haremos referencia a los dispositivos de almacenamiento masivo de la información que son los que mayor afectación presentan en la protección de los datos personales.

4.2. Los dispositivos de almacenamiento masivo de información

El registro de dispositivos de almacenamiento masivo de la información se aborda en los arts. 588 bis sexies a, b y c LECr (Capítulo VIII del Título VIII, Libro II, "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"). La regulación de este tipo de diligencia de investigación refuerza la seguridad jurídica que se necesitaba en la obtención de la prueba electrónica [37]. Se sigue la doctrina

---

[34] ROJ: STS 1594/2017 - ECLI:ES:TS:2017:1594.

[35] ROJ: STS 5362/2015 - ECLI:ES:TS:2015:5362.

[36] Así mismo, una recopilación de las sentencias más recientes de la Sala de lo Penal del TS que asientan la doctrina jurisprudencial de los medios de prueba tecnológicos la realizan Villegas García, María Ángeles / Encinar del Pozo, Miguel Ángel, "Validez de medios de prueba tecnológicos", *Diario La Ley,* Núm. 9005, Sección dossier, 21 de junio de 2017.

[37] La doctrina ponía así de relieve la necesidad de una autorización judicial expresa habilitante para poder llevar a cabo el registro de este tipo de dispositivos de almacenamiento masivo de la información. Véase entre otros, Castillejo Manzanares, Raquel, "Medios Probatorios", *Hacia un nuevo proceso penal*, *op. cit.,* "…el procedimiento adecuado en estos supuestos, esto es, cuando se trate de la inspección o recogida de dispositivos y soportes de almacenamiento masivo de datos, es que la autorización judicial debería contener expresamente su práctica y sobre qué soportes se ha de realizar". Sobre este tema podemos ver también Delgado Martín, Joaquín, "La prueba electrónica en el proceso penal", *Diario La Ley,* Núm. 8167, Sección Doctrina, 10 de octubre de 2013, González-

del TS que se incorpora a la regulación; así, entre otras muchas, la sentencia del TS 785/2008, de 25 de noviembre, F. J. 4[38]. Por lo tanto, la jurisprudencia argumentaba y en esa línea se legisla que los dispositivos de almacenamiento masivo son algo más que una pieza de convicción a aportar a los autos y que habrá que estar a su contenido, ie., se debe tener en cuenta que contienen datos de carácter personal y, por lo tanto, es necesario o bien, el consentimiento del titular o un título habilitante, ie., una resolución judicial en forma de Auto, que fije, expresamente, los términos y alcance de los dispositivos que deben ser registrados.

Los dispositivos de almacenamiento masivo pueden, además de afectar el art. 18.1 CE y el art. 18.3 CE, vulnerar el derecho a la protección de los datos personales del art. 18.4 CE. Esta diligencia de investigación resulta ser la más lesiva para los datos de carácter personal puesto que se accede a dispositivos electrónicos donde se contiene una enorme cantidad de datos personales. Ya desde la sentencia del TS 342/2013, de 17 de abril, F. J. 8, se pone de manifiesto esta circunstancia y la necesidad de autorización judicial

---

Cuéllar Serrano, Nicolás, AA.VV., "Garantías constitucionales en la persecución penal en el entorno digital", *Derecho y justicia penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuéllar García*, Colex, Madrid, España, 2006, pp. 887-916, Ortiz Pradillo, Juan Carlos, "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar probar el delito,* AAVV (coord. Pérez Gil, Julio), La Ley, 2012, pp. 267-310, Pérez Gil, Julio / González López, Juan José, "La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal", *Diario La Ley,* Núm. 8217, 2013. Cabezudo Rodríguez, Nicolás, "Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal", *Nuevos horizontes del derecho procesal: libro-homenaje al Prof. Ernesto Pedraz Peñalva* (coords. Jimeno Bulnes, Mar / Pérez Gil, Julio), Bosch, Barcelona, España, 2016, pp. 541-558.

[38] Roj: STS 7179/2008 - ECLI: ES:TS: 2008:7179. Recuerda la doctrina consolidada de la Sala "…esta Sala Segunda SSTS 985/2009 de 13.12, 342/2013 de 17.4, 587/2014 de 18.7, tiene declarado que: El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE)".

habilitante que justifique el sacrificio del titular del dispositivo a la protección de sus datos personales[39].

La importancia de esta sentencia 342/2013 radica, además, en que recoge el tratamiento jurídico que el TS realiza del contenido almacenado en el dispositivo electrónico[40]. Se decanta por la protección de "derecho al

[39] Roj: STS 2222/2013 - ECLI: ES:TS: 2013:2222. En el F. J. 8 de la STS 342/2013 se recoge: "El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones. En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal".

[40] El F. J. 8 de la STS342/2013 dice así: "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los

propio entorno virtual" que lo define como "toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Se trata de contemplar de forma unitaria mensajes, imágenes, documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado". El TS considera que este tratamiento jurídico unificado puede ser más adecuado para su protección jurisdiccional y lo denomina "derecho al propio entorno virtual" al que concede un plus de protección superior en el momento de su sacrificio que el tratamiento constitucional individualizado cada uno de los derechos contemplados en el art. 18 CE.

4.3. Ilicitud de la prueba tecnológica obtenida vulnerando el derecho fundamental a la protección de los datos de carácter personal

La protección de los datos de carácter personal elevada al rango de derecho fundamental debe traer como consecuencia en el proceso penal la ilicitud de la prueba en el caso de que los datos del investigado se hayan obtenido vulnerándolo. No obstante, esta afirmación, no existe aún doctrina jurisprudencial unívoca al respecto. Pero es que, además, en las pocas sentencias en que se trata la vulneración de los datos de carácter personal y su posible ilicitud se opta por la protección del "derecho al entorno virtual o digital" en vez de la protección, de manera aislada o individual, de los derechos del art. 18 CE.

Además de lo anterior, existen diferencias de tratamiento en la obtención de la vulnerando los datos de carácter personal. El TS distingue entre si los datos se han obtenido por un particular o si han sido aprehendidos por la policía judicial con motivo de una investigación penal. Así la sentencia del TS

---

poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías".

116/2017, de 23 de febrero[41] que, en el F. J. 6, distingue los dos supuestos: "…está fuera de discusión la necesidad de excluir el valor probatorio de aquellas diligencias que vulneren el mandato prohibitivo del art. 11 de la LOPJ. Pero más allá del fecundo debate dogmático acerca de lo que se ha llamado la eficacia horizontal de los derechos fundamentales, es evidente que la acción vulneradora del agente de la autoridad que personifica el interés del Estado en el castigo de las infracciones criminales nunca puede ser artificialmente equiparada a la acción del particular que, sin vinculación alguna con el ejercicio del ius puniendi, se hace con documentos que más tarde se convierten en fuentes de prueba que llegan a resultar, por una u otra circunstancia, determinantes para la formulación del juicio de autoría. El particular que por propia iniciativa desborda el marco jurídico que define la legitimidad del acceso a datos bancarios, ya actúe con el propósito de lograr un provecho económico, ya con el de fomentar el debate sobre los límites del secreto bancario, no lo hace en nombre del Estado. No rebasa el cuadro de garantías que define los límites constitucionales al acopio estatal de fuentes de pruebas incriminatorias. Nada tiene que ver esa actuación con la de un agente al servicio del Estado. Lo que proscribe el art. 11 de la LOPJ no es otra cosa que la obtención de pruebas (" no surtirán efecto las pruebas obtenidas..".). Es el desarrollo de la actividad probatoria en el marco de un proceso penal –entendido éste en su acepción más flexible– lo que queda afectado por la regla de exclusión cuando se erosiona el contenido material de derechos o libertades fundamentales". Es interesante en este tema, aunque no es objeto de estudio del trabajo, la evolución jurisprudencial de la doctrina de la prueba ilícita. Dentro de los sistemas de exclusión de la prueba ilícita el TC y el TS se decantan por la ilicitud de la prueba obtenida por los agentes de la autoridad utilizando conductas que afectan derechos fundamentales, pero admitiendo la obtenida por el particular de manera ilícita vulnerando los derechos fundamentales[42].

---

41 Roj: STS 471/2017 - ECLI: ES:TS:2017:471.

42 Parece que no se trata tanto de proteger los derechos fundamentales sino de evitar conductas policiales ilícitas destinadas a conseguir pruebas incriminatorias. Siguiendo los precedentes del Tribunal Supremo Norteamericano (ya desde el caso Burdeu vs Macdowell, 1921) la reciente sentencia del TS 116/2017, "Lista Falciani", sigue esa tesis; admite valorar la prueba obtenida violentando el derecho fundamental a la intimidad al haberse obtenido por un particular y no por agente de autoridad y no resultar una violación grave. El peligro de esta línea jurisprudencial es dejar que el particular recopile pruebas incriminatorias sin necesidad de resolución judicial que habilite obtenerlas. Un estudio de los orígenes y evolución de la prueba ilícita lo realizan Zaragoza Tejada, Javier Ignacio / Gutierrez Azanza, Diego Alberto, "La prueba ilícita, Una reflexión tras la STS del 23 de febrero de 2017" *Revista Aranzadi de Derecho y Proceso Penal,* Núm. 47, 2017. Como bien recuerda Asensio Mellado, José María, "La prueba ilícita en el proceso civil tras la STS 116/2017, de 23 de febrero, dictada en el llamado caso Falciani", *Práctica de Tribunales,*

La doctrina se empieza a plantear la repercusión que tiene en el proceso penal la vulneración del derecho a la protección de los datos personales del sujeto investigado. Se ponen de manifiesto las consecuencias que en el proceso penal debe tener la obtención, de manera ilícita, de datos personales del investigado y su incidencia en la valoración de la prueba[43]. Incluso, se va más allá al cuestionarse el tratamiento jurisdiccional que se otorga a los datos personales en "…el período que transcurre entre la obtención y la celebración del juicio oral"[44]. Se habla entonces de garantizar la integridad de los datos durante la tramitación del proceso penal[45]. Se podía haber aprovechado la reforma de la legislación procesal en materia de medidas de investigación tecnológica para realizar una protección específica del derecho a la protección de los datos personales cuando resulten afectados por la obtención de prueba tecnológica.

Núm. 135, Noviembre-Diciembre, el sistema anglosajón es diferente a nuestro modelo procesal al igual que lo es el origen de nuestros tribunales por lo que aceptar o traspasar directamente ese modelo supone, en palabras del autor, "una degradación de la prueba ilícita". En el mismo sentido Fuentes Soriano, Olga, "Vídeos, comunicación electrónica y redes sociales: cuestiones probatorias", *Práctica de Tribunales*, Núm. 135, Noviembre-Diciembre, cuando constata el distinto alcance de la regla de exclusión probatoria en los órdenes jurisdiccionales laboral y penal evidencia, en palabras de la autora "…el fracaso alcanzado en la aplicación del art. 11.1 LOPJ cuyo objetivo último, se supone, es garantizar la preeminencia de los derechos fundamentales en el ordenamiento y preservarlos frente a posibles injerencias".

43 Así lo cuestiona Gutiérrez Zarza, Ángeles, "La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?", *La Ley penal*, Núm. 71, mayo 2010, Protección de Datos en el Proceso Penal, p. 4 que entiende que la protección de los datos personales debe formar parte del conjunto de principios y derechos del proceso penal.

44 Esparza Leibar, Iñaki, "Protección de datos de carácter personal y proceso penal" ponencia presentada en el Congreso *El nuevo proceso penal sin código procesal penal*, celebrado en la Universidad de Santiago de Compostela, los días 9 y 10 de noviembre de 2017.

45 Delgado Martín, Joaquín, "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", *Diario La Ley,* Núm. 8693, Sección doctrina, 2 de febrero de 2016, p. 3, destaca el problema de la manipulación de los datos: "…los datos pueden ser fácilmente modificados, sobre-escritos o borrados, lo que determina un peligro evidente de manipulación de las pruebas. De esta forma resulta necesario utilizar técnicas que permitan obtener dichos datos y garantizar su autenticidad e integridad durante la tramitación del proceso (cadena de custodia)". Las consecuencias en el proceso penal de los datos personales obtenidos violentando este derecho fundamental también lo pone de relieve Frías Martínez, Emilio, "Protección y tratamiento de datos personales por el Ministerio Fiscal", *La Ley penal,* Núm. 71, mayo 2010, Protección de datos en el proceso penal, p. 7, quien no duda de la ilicitud de la prueba así obtenida: "Al elevar la protección de los datos de carácter personal a la categoría de derecho fundamental, la ilicitud en la obtención de los mismos tendrá consecuencias directas en la consideración de su valor probatorio, pues indudablemente los datos que hayan sido obtenidos con quebranto del derecho fundamental no podrán ser valorados para desvirtuar la presunción de inocencia".

No existe en este tema aún pronunciamiento jurisprudencial claro sobre las consecuencias en el proceso penal de la vulneración del derecho de protección de datos personales ni de los relativos a la salud. En cualquier caso, el acceso, a efectos probatorios, a datos personales de todo tipo en el entorno virtual, que revelan el perfil personal del investigado, se ha de convertir en uno de los retos que deberán protegerse desde el ámbito de las garantías procesales[46].

[46] En el caso del consentimiento del investigado para el acceso a su entorno virtual la LECr no regula las condiciones en que se debe prestar ese consentimiento para que tenga validez en el proceso. Podemos ver un estudio de esta problemática realizado por Fernández – Gallardo Fernández – Gallardo, Javier Ángel, *La Ley Penal,* Núm. 126, Sección Legislación aplicada a la práctica, mayo-junio 2017.

Transferencias internacionales de datos genéticos y datos de salud con fines de investigación*

International transfers of genetic data and health data for research purposes

Mikel Recuero Linares

Investigador G.I. Cátedra de Derecho y Genoma Humano, Departamento de Derecho Público, Universidad del País Vasco UPV/EHU (Bilbao, España)

DOI: 10.14679/1143

Sumario / Summary: 1. Introducción. 2. Concepto y definición de transferencia internacional de datos. 3. Régimen jurídico aplicable a las transferencias internacionales de datos desde Estados de la Unión Europea a terceros países u organizaciones internacionales. 4. Mecanismos y vías para la realización de transferencias internacionales de datos genéticos y de salud con fines de investigación. 4.1. Transferencias basadas en una decisión de adecuación (art. 45). 4.2. Transferencias mediante garantías adecuadas (arts. 46 y 47). 4.3. Excepciones para situaciones específicas (art. 49). 5. Consideraciones finales y propuestas. 5.1. Primera propuesta: un código de conducta para la investigación en salud. 5.2.

* Artículo recibido el 1 de septiembre de 2019 y aceptado para su publicación el 20 de septiembre de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos -*Big Data*-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER). Asimismo, este trabajo se ha realizado en el marco del Proyecto PMP17/00007 *Functional and Clinical Impact of Genomic Analysis in CLL*, integrado en el Plan Estatal de I+D+I y cofinanciado por el ISCIII-Subdirección General de Evaluación y el Fondo Europeo de Desarrollo Regional (FEDER - "Una manera de Hacer Europa") y se ha contado con la ayuda concedida por el Departamento de Educación del Gobierno Vasco para apoyar las actividades del Grupo de Investigación de la Cátedra de Derecho y Genoma Humano (Ref. nº IT1066-16).

Segunda propuesta: cooperación internacional, consorcios y organizaciones. 5.3. Tercera propuesta: a falta de *hard law, soft law*. 6. Bibliografía.7. Normativa citada.

Resumen / Abstract: El desarrollo presente y futuro de la investigación científica y, en especial, la biomédica, depende, en gran medida, de la internacionalización del sector y de la constitución de un ecosistema científico global y conectado. Sin embargo, el procesamiento y tratamiento de grandes cantidades de datos personales (*big* data), unida a las transferencias internacionales de estos datos plantean una serie de interrogantes y retos para la protección de datos de carácter personal. Por consiguiente, el presente artículo pretende identificar las carencias y virtudes del actual marco jurídico de protección de datos personales en relación a la puesta en marcha de proyectos y consorcios paneuropeos e internacionales de investigación que requieren la recogida, explotación y re-utilización de grandes cantidades de datos genéticos y de salud, así como presentar los diversos mecanismos y soluciones susceptibles de ser utilizados para la consecución de dicha finalidad.

The development of scientific research and, in particular, the biomedical research, depends on the internationalisation of this sector and the creation of a global and connected scientific ecosystem. However, the processing of large amounts of personal data (big data) together with the international transfers of such data raises a number of questions and challenges. Therefore, this article aims to identify the shortcomings and virtues of current legal framework of data protection in relation to the creation of pan-european and international research projects and consortia. Specially, those that require the collection, processing and re-use of large amounts of genetic data and data concerning health.

Palabras clave / Keywords:

Transferencias internacionales / circulación de datos / datos personales / datos genéticos / datos de salud / datos sensibles / categorías especiales / investigación científica / investigación biomédica / macrodatos / códigos de conducta / certificación.

Transfers of personal data / personal data / genetic data / data concerning health / sensitive data / special categories / scientific research / biomedical research / big data / codes of conduct certification.

1. Introducción

La utilización del *big data* en la investigación científica y, en especial, la biomédica, no solo se ha consolidado, sino que se ha erigido como una suerte de necesidad contemporánea para el progreso de la medicina. Los potenciales beneficios que del procesamiento masivo de datos genéticos y de salud pueden proyectarse, por ejemplo, para la predicción de futuras epidemias o emergencias sanitarias de la población, para la determinación de posibles efectos adversos de medicamentos o incluso para el desarrollo más rápido y menos costoso de nuevos fármacos o procesos asistenciales son indiscutibles. Tanto es así que el propio Reglamento General de Protec-

ción de Datos[1] (en lo sucesivo, RGPD), siendo consciente de esta realidad, reconoce el valor que el empleo de grandes cantidades de datos e incluso, la combinación de información procedente de diversos registros, puede tener para los investigadores a la hora de obtener nuevos conocimientos sobre condiciones médicas extendidas[2]. Sin embargo, el hecho de procesar datos a gran escala revelados por pacientes o sujetos con otras finalidades que no hubieran pretendido o previsto primigeniamente representa un evidente reto para los principios tradicionales de la protección de datos de carácter personal. Así pues, resulta imprescindible conciliar dos intereses en principio antagónicos: el alto valor de esa información para la investigación científica y los derechos de los individuos respecto a sus datos de carácter personal[3].

El segundo gran desafío es la proliferación de un contexto científico global y conectado en el que las transferencias internacionales de datos se constituyen como una herramienta indispensable para la puesta en marcha de proyectos y consorcios paneuropeos e internacionales de investigación que requieren la recogida, explotación y re-utilización de grandes cantidades de datos genéticos y de salud. Con la ardua encomienda de procurar un equilibrio entre, por un lado, la libre circulación internacional de datos genéticos y de salud en pos de la investigación científica y, por otro, la salvaguarda del derecho fundamental a la protección de datos personales ve la luz el RGPD[4]. Cabe preguntarse, por ende, si las soluciones aportadas por la nueva norma son adecuadas para dotar al sector de la investigación del anhelado y tan necesario marco común y global o si, por el contrario, el reforzamiento de los derechos y garantías de las personas físicas puede haber terminado desincentivado la inversión y el desarrollo de aquél.

Así, mientras que la primera de las cuestiones referidas *supra* ha sido abordada profusamente por la doctrina, en lo que se refiere a los retos que plantean para la protección de datos personales la internacionalización de

---

1 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 circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE, L 119/1, 04/05/2016).

2 Vid. Considerando 157 del RGPD.

3 Miralles López, R., "Desvinculando datos personales: seudonimización, desidentificación y anonimización", *I+S: Revista de la Sociedad Española de Informática y Salud* [en línea]. Madrid: Sociedad Informática de la Salud, Núm. 122, abril 2017. p. 7. [Última consulta: 13 de julio de 2019].

4 No es baladí que la circulación de los datos personales ocupe una posición fundamental entre los objetivos y prioridades del Reglamento, en pos del desarrollo de un ecosistema de datos global en ámbitos como el económico, el científico o el académico y la explotación de sus potenciales beneficios.

la investigación y el ecosistema científico global son pocas las voces que se han pronunciado. Por consiguiente, el presente artículo ambiciona ofrecer una visión general de los diversos mecanismos susceptibles de ser utilizados para intercambiar y transferir internacionalmente datos personales genéticos y datos relativos a la salud con fines de investigación, en aras a la constitución de proyectos y consorcios de investigación a nivel paneuropeo e internacional.

La relevancia y la necesidad de compartir y transferir datos a nivel internacional no es algo disruptivo de las sociedades globales e interconectadas del s. XXI. Ya en el año 1980 la Organización para la Cooperación y el Desarrollo Económicos (en lo sucesivo, OCDE) publicaba unas Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales[5] en las que destacaba la importancia de dichos flujos e instaba a los Estados parte a no restringir el intercambio transfronterizo de datos con los demás Estados miembros. Tan solo un año después, el Consejo de Europa, por medio del Convenio nº 108[6], confirmaba la necesidad de que las transferencias internacionales de datos estuvieran generalmente autorizadas.

Sin embargo, lo cierto es que esta tendencia a la globalización de los datos se ha tornado, si cabe, más acuciante, con el advenimiento de las nuevas Tecnologías de la Información y la Comunicación y, en especial, de Internet. La aplicación de las nuevas tecnologías de computación masiva como el *big data* han facultado intercambios simultáneos y procesamientos en tiempo real, abriendo un nuevo horizonte para la investigación científica y biomédica. Ello, unido al acceso transnacional a los datos resulta determinante para el éxito del estudio y la revelación de bases genéticas de enfermedades como el cáncer. Valga como ilustración el impulso de la propia Comisión Europea para el desarrollo de proyectos paneuropeos como *1+Million Genomes*[7] e internacionales como *EUCANCAN*[8] que ambicionan la generación de un mar-

[5] Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (OCDE, 23 de septiembre de 1980).

[6] Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 28.I.1981)

[7] Iniciativa que pretende ofrecer acceso a al menos 1 millón de genomas secuenciados en la UE para 2022, articulando un mecanismo de colaboración (una red federada de acceso) entre Estados europeos que permita y fomente el desarrollo de la medicina personalizada y nuevos impulsos a la investigación traslacional que se traduzca en resultados clínicos y tangibles para la población.

[8] Proyecto de cooperación entre la UE y Canadá cuyo objeto es establecer un marco legal, ético y tecnológico integrado para compartir y gestionar datos genómicos sobre el cáncer que faciliten la investigación biomédica y el aprovechamiento de sus avances en los sistemas públicos de salud. Para más información sobre el proyecto puede consultarse la web: http://eucancan.com/about/

co legal y ético común para compartir y acceder supranacionalmente a datos genéticos y datos de salud con fines de investigación científica y biomédica.

2. Concepto y definición de transferencia internacional de datos

El primer escollo por soslayar es la propia definición y conceptualización de transferencia internacional, pues ni la anterior Directiva de Protección de Datos de 1995[9] (en lo sucesivo, DPD), ni el RGPD en la actualidad expresan qué se entiende como tal. Sí lo definía, en cambio, el art. 5.1.s) del Reglamento de la Ley Orgánica de Protección de Datos, todavía hoy vigente[10], que consideraba transferencia internacional el "tratamiento de datos que supone la transmisión de estos fuera del territorio del Espacio Económico Europeo". Esta alusión al Espacio Económico Europeo (en adelante, EEE) es actualmente incorrecta, pues los países del EEE también deben ser considerados países terceros, debido a que el propio RGPD no les excluye en ningún momento de dicha consideración[11]. Así, tal y como propone el mismo autor, por transferencia internacional debe entenderse "un tratamiento de datos en el que hay implicado, al menos, un Estado miembro de la UE y un país tercero (de fuera de la UE) o una organización internacional"[12]. La alusión explícita a organización internacional es reseñable, en tanto en cuanto sí se halla definida expresamente en el Reglamento[13].

La aproximación conceptual realizada debe ser contemplada, asimismo, a la luz de la jurisprudencia del TJUE, que ha precisado que la difusión de datos personales en una página web realizada por un interesado ubicado en un Estado miembro no se considerará una transferencia internacional,

---

9 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE, nº L 281/31, del 23/11/95).

10 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17). No se define, tampoco, transferencia internacional, en la vigente LOPDyGDD.

11 Piñar Mañas, J. L., "Las transferencias internacionales en el nuevo reglamento europeo de protección de datos", *Los retos del Estado y la Administración en el siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo*, Vida Fernández, J. / Parejo Alfonso, L.J. (Coords.). Ed. Tirant lo Blanch, Valencia, España, Vol. 2, 2017. p. 2063.

12 *Ídem*.

13 *Vid*. Art. 4.26. "organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo".

ni siquiera, aunque dichos datos sean accesibles a través de Internet por personas de terceros países[14].

Otra cuestión controvertida es la relativa a la situación en la que quedará el Reino Unido si se termina materializando un *Brexit* sin acuerdo. A juicio del Comité Europeo de Protección de Datos (CEPD), Reino Unido pasará a ser considerado un tercer país[15], lo que significa que sólo podrán realizarse transferencias internacionales de datos con Estados de la UE a través de los mecanismos de garantías adecuadas[16].

3. Régimen jurídico aplicable a las transferencias internacionales de datos desde Estados de la Unión Europea a terceros países u organizaciones internacionales

Esclarecido, al menos en parte, el concepto de transferencia internacional, procede ahora realizar sucinta alusión al régimen general previsto en el RGPD. La mención al "régimen general" no es casual. Se debe a que el Reglamento no contiene ninguna disposición que se ocupe específicamente de las transferencias internacionales de datos con fines de investigación científica. Esto es, sin perjuicio de las especialidades que contiene el RGPD respecto a la recogida y tratamiento de datos genéticos y de salud con fines de investigación –que difiere en algunos extremos de los principios generales proclamados–, el régimen de transferencias internacionales de datos contenido en los arts. 44 a 50 del RGPD resulta aplicable a la generalidad de los tratamientos sometidos al Reglamento.

Esta opción legislativa ofrece como gran virtud la aplicación de un régimen armonizado y uniforme para todos los Estados miembros –sin apenas divergencias entre normativas internas– mas, en contraposición, no permite tener en cuenta las características y necesidades propias del sector de la investigación científica y biomédica. Por consiguiente, resulta pertinente abordar los cauces por los que los datos genéticos y de salud podrían circular a nivel internacional entre consorcios y proyectos de investigación, pero aplicando

[14] STJUE de 6 de noviembre de 2003, Caso *Bodil Lindqvist*, Asunto C-101/01.

[15] *Information note on data transfers under the GDPR in the event of a no-deal Brexit* (Comité Europeo de Protección de Datos, 12 de febrero de 2019).

[16] Puede leerse más sobre las consecuencias del Brexit para las transferencias internacionales de datos genéticos en: Taylor, M. J. / Wallace, S. E. / Prictor, M., "United Kingdom: transfers of genomic data to third countries", *Human Genetics,* Núm. 8, Vol. 137, 2018.

las normas generales de las transferencias internacionales del Capítulo V del Reglamento (arts. 44 a 50).

Dichas disposiciones no son, ciertamente, de nuevo cuño, pues textos como los ya indicados de la OCDE y del Consejo de Europa pergeñaban unos principios similares, ratificados más tarde en la propia DPD. En la actualidad, por ende, la esencia del RGPD no dista mucho del enfoque primigenio de la derogada Directiva: solo podrán transferirse datos personales a terceros países u organizaciones internacionales cuando el nivel de protección de las personas físicas garantizado en el propio Reglamento no se vea menoscabado[17]. Sin embargo, la nueva regulación, además de ser más sistemática y extensa que la de su predecesora, también introduce dos importantes novedades (junto a la ya referida mención expresa a las organizaciones internacionales).

En primer lugar, de la interpretación conjunta del Considerando 101 y del art. 44 se infiere la aplicación del régimen tanto a responsables como a encargados del tratamiento, pero no solo a las transferencias iniciales, sino también a las ulteriores que éstos pudieran efectuar a otros países u organizaciones. Esta previsión es muy significativa en tanto en cuanto el destinatario de los datos no sólo deberá acreditar o garantizar que cumple con el nivel de protección del Reglamento, sino que además, deberá cerciorarse de que cualquier encargado o responsable al que vaya a ceder o comunicar esos datos también lo haga.

En segundo lugar, sin perjuicio de otras previsiones novedosas[18], el último aspecto a remarcar del régimen jurídico de las transferencias internacionales contenido en el Reglamento es la apertura de nuevas vías para su realización y, en especial, la ampliación del número y la naturaleza de los instrumentos para el ofrecimiento de garantías adecuadas, incluso sin autorización de las entidades de supervisión[19]. Por tanto, en la actualidad, podrán efectuarse

[17] Art. 44 *in fine* del RGPD.

[18] Como por ejemplo, el deber de informar al interesado sobre las transferencias (que además podrá ser excepcionado en determinados tratamientos con fines de investigación científica de conformidad con el art. 14.5.b), la llevanza de un registro de actividades de tratamiento con indicación de las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales con inclusión de "los destinatarios en terceros países u organizaciones internacionales" (art. 14.1d) y la tipificación como sanción de los incumplimientos de los arts. 44 a 49 con multas de hasta 20 mill. o el 4% del negocio anual.

[19] García, R. "El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario", *I+S: Revista de la Sociedad Española de Informática y Salud,* Sociedad Informática de la Salud, Núm. 127, 2018, pp. 13-20. Disponible en: https://seis.es/revista-no-127/ [Última consulta: 14 de julio de 2019].

transferencias internacionales de datos a un tercer país o a una organización internacional en tres supuestos: cuando se basen en una decisión de adecuación, cuando se ofrezcan garantías adecuadas o cuando encuentren amparadas en alguna de las excepciones del art. 49.

4. Mecanismos y vías para la realización de transferencias internacionales de datos genéticos y de salud con fines de investigación

Como acaba de aludirse, el Reglamento posibilita tres vías o cauces para la realización de transferencias internacionales de datos, aunque la doctrina señala que solo dos de ellas son apropiadas para proyectos o consorcios colaborativos de investigación científica a nivel internacional[20]. Empero, en lugar de examinar teóricamente el compendio de mecanismos proporcionados por la norma comunitaria[21], se propone, en su lugar, un análisis casuístico limitado a aquellas alternativas que pudieran resultar viables en la práctica para realizar las meritadas transferencias e intercambios internacionales de datos.

Así pues, se plantean, fundamentalmente, dos vías para la realización de las transferencias internacionales de datos genéticos y de salud con fines de investigación: las basadas en una decisión de la Comisión y las basadas en el otorgamiento de garantías adecuadas (con los instrumentos a los que ahora se hará referencia). Sin perjuicio de ello, también se realizará somera referencia a las excepciones del art. 49, que han generado algunas dudas interpretativas pero que deben ser rechazadas como un cauce óptimo para la antedicha finalidad.

4.1. Transferencias basadas en una decisión de adecuación (art. 45)

Se trata del primer supuesto habilitado por el Reglamento y, según la doctrina mayoritaria, la vía más cómoda, directa y sencilla para compartir y transferir datos internacionalmente con fines de investigación[22], sin perjuicio

[20] Slokenberga, S. "Biobanking between the EU and Third Countries: Can Data Sharing Be Facilitated via Soft Regulatory Tools?", *European Journal of Health Law*, Núm. 5, Vol. 25, Brill, Holanda, p. 526. [Última consulta: 21 de junio de 2019].

[21] Cuestión ya abordada profusamente por la doctrina y que implicaría una reproducción cuasi-literal del propio articulado del Reglamento.

[22] *Vid*. entre otros: Manis, M. L. "The processing of personal data in the context of scientific research: the new regime under the EU-GDPR", *BioLaw Journal*, Núm. 3, 2017, p. 350. [Última consulta: 15 de junio de 2019] y Gonzalo Domenech, J.J., "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y

de una serie de matizaciones que a continuación se realizarán. Implica, básicamente, que se podrá realizar la transferencia si la Comisión, a través de una Decisión, ha decretado que un tercer país, uno o varios territorios o sectores específicos de ese país o una organización internacional garantizan un nivel de protección adecuado. Para valorar este nivel de adecuación el propio Reglamento expresa unos criterios como el Estado de derecho, los derechos humanos, la existencia de autoridades de control independientes o los compromisos internacionales asumidos[23].

Las ventajas de recurrir a este mecanismo resultan palmarias. La Decisión tendrá efectos para toda la Unión (Considerando núm. 103) y no se requerirá ninguna autorización específica (art. 45.1 *in fine*). Además, se presenta como un mecanismo flexible y adaptable, pues permitiría limitar los efectos jurídicos inherentes a la declaración del nivel de adecuación a determinados territorios o incluso determinados sectores. Consecuentemente, se erige como una opción efectivamente viable en la práctica, pues por medio de una Decisión la Comisión podría decretar que uno o varios países u organizaciones presentan el nivel de protección adecuado, pero limitando dichos efectos al sector de la investigación científica en general o, incluso, de la investigación biomédica en particular.

En contraposición a lo anterior, este cauce presenta, fundamentalmente, tres defectos[24]. En primer lugar, existen a día de hoy, muy pocos Estados con una Decisión de adecuación[25] que, además, mayoritariamente, han sido aprobadas al amparo de las disposiciones de la ya derogada DPD[26]. En segundo lugar, algunas de estos actos de ejecución no se aplican a todos los tratamientos[27] o se limitan a los sujetos o entidades adheridas expresamente a dichos

---

los mecanismos de control aplicados por los Estados Miembros". *Cuadernos de derecho transnacional*, Núm. 1, Vol. 11, 2019, p. 355 [Última consulta: 21 de junio de 2019].

23 *Vid.* art. 45.2 y Considerandos núm. 104 y 105.

24 Señalados, entre otros, por: Phillips, M. "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)", *Human Genetics*, Núm. 8, Vol. 137, 2018, p. 579.

25 A saber: Argentina, Canadá (régimen limitado), Suiza, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Estados Unidos.

26 El art. 45.9 del RGPD establece que las Decisiones adoptadas por la Comisión en virtud de las disposiciones de la DPD "permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas".

27 Es el caso concreto de la Decisión 2002/02/CE, de 20 de noviembre de 2001, con Canadá, que únicamente cubre los tratamientos de datos personales sujetos a la ley federal *Personal Information and Electronic Documents Act*, que se aplica a las entidades privadas que utilicen datos con fines comerciales, aunque también se alude a su aplicación a los datos sanitarios. En este sentido, el GT29 (Dictamen 2/2001, de 26 de enero de 2001) ha

mecanismos[28]. Por último, en tercer lugar, tras el pronunciamiento del TJUE en el Caso *Schrems*[29], por el que se anulaba la Decisión *Safe Harbor* entre la UE y EEUU, se ha sembrado un cierto halo de sospecha e incertidumbre en relación a la verdadera valoración de los niveles de adecuación y de la efectividad práctica de los mecanismos establecidos para su cumplimiento y verificación. La referida sentencia no solo trajo consigo la declaración de invalidez de la Decisión de adecuación *Safe Harbor* entre EEUU y la UE[30]. Junto a ello, el TJUE confirmó que las autoridades de protección de datos nacionales eran plenamente competentes para acudir a los tribunales nacionales e incluso para promover cuestiones prejudiciales, además de abogar por la revisión periódica del cumplimiento y la viabilidad de las Decisiones por la propia Comisión[31].

En conclusión, podría emplearse como un mecanismo verdaderamente útil para fundamentar las transferencias internacionales con fines de investigación científica, teniendo en cuenta las deficiencias señaladas y su repercusión práctica que, en definitiva, convertirían el mecanismo de las Decisiones en una suerte de "presunción de garantías"[32] que cabe ser destruida mediante prueba en contrario –a través de su impugnación ante el TJUE con la correspondiente cuestión prejudicial–.

4.2. Transferencias mediante garantías adecuadas (arts. 46 y 47)

En ausencia de una Decisión de la Comisión sobre el nivel de adecuación de un determinado país u organización (art. 46.1 y Considerando núm. 108 del RGPD) y, por ende, como segunda opción posible, el responsable o encargado podrá transferir los datos únicamente cuando ofrezca garantías adecuadas para el interesado. Sin embargo, no es suficiente con ofrecer dichas garantías sino que además, el propio art. 46.1 *in fine* exige "que los interesados cuenten con derechos exigibles y acciones legales efectivas".

---

criticado la escasa atención y protección especial que la meritada ley dispensa a los datos sensibles como son los datos relativos a la salud y los datos genéticos.

[28] En el caso de la Decisión 2016/1250, de 12 de julio de 2016 con Estados Unidos, mediante la que se establece el llamado *Privacy Shield*, tras la anulación del anterior acuerdo *Safe Harbor* por el TJUE.

[29] STJUE de 6 de octubre de 2015, Caso *Schrems*, Asunto C-362/14.

[30] El TJUE entendió que la existencia de una norma estadounidense que permitía a sus autoridades públicas acceder de manera indiscriminada e ilimitada al contenido de las comunicaciones electrónicas de ciudadanos europeos (tras las revelaciones del Caso *Snowden*) lesionaba el derecho a la protección de datos y denotaba que no se estaba ofreciendo un nivel adecuado de garantías para aquéllos.

[31] A raíz del pronunciamiento del Caso *Schrems*, estas dos cuestiones se han incorporado expresamente al articulado del Reglamento (vid. arts. 45.4, 45.5 y 58.5, entre otros).

[32] Gonzalo Domenech, J. J. "Las decisiones de adecuación… *op. cit.* p. 355.

Este último requisito resulta problemático en la práctica, pues el RGPD, salvando una pequeña mención en el Considerando núm. 108[33], no ofrece una definición o lista exhaustiva, siendo preciso realizar un análisis casuístico, que en el caso de la investigación científica puede antojarse excesivamente complejo debido a las divergencias que existen en el régimen de derechos de los interesados por su remisión a los Estados miembros. A este respecto, el GT29 ha venido señalando que habrá de valorarse individualmente el nivel de riesgo de las transferencias o tratamientos –por lo que, necesariamente, se deberá tener presente el carácter sensible de los datos personales genéticos y de salud– para adoptar las medidas que sean efectivas para cada caso concreto[34]. Así pues, de todo ello podría concluirse que, además de optar por alguno de los instrumentos para el otorgamiento de garantías adecuadas que ahora se expondrán, lo recomendable sería efectuar un análisis de riesgo o, incluso, una evaluación de impacto antes de realizar el correspondiente tratamiento y transferencia de datos con fines de investigación.

El Reglamento, actualmente, permite otorgar estas garantías adecuadas a través de una pluralidad de instrumentos que pueden agruparse en dos grandes bloques: las que no requieren autorización expresa de una autoridad de control (art. 46.2) y las que sí exigen autorización de la autoridad competente (art. 46.3). En lo que se refiere a las primeras, las no necesitadas de autorización, la norma menciona las siguientes:

– *Instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos (art. 46.3.a).* Su utilización parece estar circunscrita y limitada –al margen del escaso desarrollo y concreción– a las relaciones entre organismos y autoridades públicas lo que, en principio, desaconsejaría su empleo generalizado por consorcios internacionales de investigación.

– *Normas corporativas vinculantes (arts. 46.3.b y 47).* Aunque son instrumentos jurídicamente vinculantes cuyo empleo ha sido recomendado por la propia Comisión, sirven principalmente para grandes compañías multinacionales o grupos de empresas que necesitan transferir internacionalmente datos personales entre sus divisiones

[33] Establece que las acciones legales efectivas incluirían "el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la UE o en un tercer país".

[34] Working Document on "Transfers of personal data to third countries: Applying articles 25 and 26 of the EU Data Protection Directive" (Grupo de Trabajo art. 29, WP 12, 24 de julio de 1998).

internas. Esto, unido a la elevada inversión inicial que requieren, las revisten de poca o nada aplicabilidad práctica en los casos de consorcios o proyectos de investigación biomédica o genómica.

– *Cláusulas tipo de protección de datos adoptadas por la Comisión (art. 46.3.c) o adoptadas por una autoridad de control y aprobadas por la Comisión (art. 46.3.d).* Se trata de auténticas disposiciones contractuales que rigen las relaciones entre los importadores y exportadores de los datos, sean responsables[35] o encargados del tratamiento[36]. Es uno de los mecanismos más utilizados en la práctica para realizar transferencias internacionales con países u organizaciones con los que no existen Decisiones. Por consiguiente, son una vía perfectamente viable (que además no requiere autorización) para compartir internacionalmente datos genéticos y de salud con fines de investigación desde el punto de vista meramente legal. Empero, esto, a su vez, puede implicar que no se valoren ni adecuadamente ni caso por caso los riesgos que entrañan los tratamientos de datos sensibles –como es el caso de los datos personales genéticos y de salud– lo que podría llegar a ser cuestionable también desde el punto de vista ético de la investigación.

– *Códigos de conducta (arts. 46.3.e y 40).* Salvando ciertos inconvenientes como que no existen todavía Códigos aprobados con el nuevo régimen del Reglamento y que requieren para su aprobación un procedimiento específico[37], constituye la alternativa más viable y completa para desarrollar correctamente proyectos y consorcios de investigación que requieran compartir grandes cantidades de datos a nivel internacional. Esto se debe a que su adopción permitiría adaptar y clarificar sus disposiciones al contexto particular de la investigación científica y biomédica[38]. Además, tendrían una

[35] Decisión de la Comisión 2001/497/CE, de 15 de junio de 2001, modificada por la Decisión 2004/915/CE, de 27 de diciembre de 2004.

[36] Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010.

[37] Dicho procedimiento, regulado en el artículo 40, podría antojarse complejo para pequeños grupos de investigación, pues requiere un procedimiento de consulta previa, la creación y acreditación de una entidad independiente supervisora de su cumplimiento (art. 41) y, finalmente, la aprobación, registro y publicidad por parte de la Comisión (art. 40.10). Sin embargo, su elaboración e impulso sectorial, desde organizaciones y asociaciones representativas en el ámbito de la investigación biomédica, unida a su eventual eficacia general (art. 40.9) podrían convertirlo en un auténtico estándar a seguir para todas los consorcios, grupos o proyectos de investigación.

[38] Phillips, M. "International data-sharing norms… *op. cit.* p. 580 y art. 40.1 del RGPD.

doble utilidad: legitimar los tratamientos de datos completando y armonizando las cuestiones controvertidas referidas a la recogida y uso de datos con fines de investigación (arts. 9 y 89.1 entre otros) y, a su vez, otorgar las garantías adecuadas para transferir los datos a un tercer país u organización internacional. Consecuentemente, a falta de una Decisión de la Comisión adoptada de conformidad con el art. 45, se configura como la mejor alternativa para articular de manera estable transferencias internacionales de datos genéticos y de salud por parte de consorcios u organizaciones paneuropeas o internacionales.

– *Mecanismos de certificación (arts. 46.3.f y 42).* Al igual que los Códigos, todavía generan ciertas reticencias e incertidumbre debido a la falta de precedentes significativos en el ámbito de la investigación (unido a que algunos Estados miembros todavía no han materializado sus procedimientos ni organismos de certificación). Al margen de ello, constituyen otra vía perfectamente posible, aunque, quizás, no tan completa como los Códigos y sin la ventaja añadida de eficacia general para el sector que la Comisión puede otorgar a estos.

En segundo lugar, en lo que concierne a los supuestos del art. 46.3, esto es, los mecanismos de otorgamiento de garantías que sí requieren autorización de la autoridad de control competente, el Reglamento alude únicamente a dos:

– *Otras cláusulas contractuales entre responsable, encargado o destinatario (art. 46.3.a).* El propio RGPD señala que el recurso a cláusulas tipo no priva a los sujetos de las transferencias de incorporar sus propias disposiciones contractuales o, incluso, de añadir las cláusulas tipo a un acuerdo más amplio (Considerando núm. 109 del RGPD). No obstante, exigen la aprobación de la autoridad de control, camino muchas veces tortuoso cuya aplicabilidad práctica cabe cuestionarse en la medida en que es posible acogerse simplemente a las cláusulas tipo y prescindir de dicha autorización[39].

– *Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos*

[39] Guasch portas, V. "La computación en nube y las transferencias internacionales de datos en el nuevo Reglamento de la UE", *Revista de Derecho UNED*, Núm. 20, 2017. Disponible en: http://revistas.uned.es/index.php/RDUNED/article/view/19471/16307, p. 343. [Última consulta: 17 de julio de 2019].

y exigibles para los interesados (art. 46.3.b). La propia mención a acuerdos administrativos y a las autoridades y organismos públicos parece suficiente para descartarlo como un mecanismo generalmente apto y útil para el presente caso.

En la práctica, el recurso a cualquiera de los dos instrumentos anteriores se antoja complicado para la articulación de transferencias internacionales con fines de investigación y la puesta en marcha de consorcios y proyectos de colaboración, debido a que exigen una aprobación previa por parte de la autoridad que puede retrasar y encarecer considerablemente la puesta en marcha del mismo. Por tanto, como ya ha sido advertido, sería preferible, más rápido y efectivo acudir a mecanismos como los códigos de conducta, certificaciones o cláusulas tipo como vías de otorgamiento de garantías adecuadas para efectuar las transferencias.

4.3. Excepciones para situaciones específicas (art. 49)

Para finalizar, es preciso realizar una somera alusión a determinadas situaciones específicas en las que la transferencia internacional podría realizarse, aun sin contar con una Decisión de adecuación y en ausencia de garantías adecuadas. En términos generales, parece improbable que en la práctica puedan servir para realizar transferencias de datos genéticos y de salud con fines de investigación, pues se trata de excepciones que deben interpretarse restrictivamente, de forma que no se conviertan en la regla[40]. Además, en caso de no poder incardinarse expresamente en ninguno de los supuestos del art. 49.1 se exigiría que se trate de transferencias no repetitivas y que afecten a un grupo limitado de interesados, lo cual, en el ámbito de la investigación científica, no parece ni probable ni viable[41]. Pese a todo, se refieren a continuación, sucintamente, tres supuestos que han planteado dudas sobre su aplicabilidad a la materia objeto del presente artículo, aunque debiendo anticiparse que, *a priori*, ninguna de ellas constituiría una opción apta o conveniente en la práctica.

En primer lugar, el art. 49.1 letra a) facultaría al responsable a realizar la transferencia cuando el interesado hubiese dado su consentimiento explícito

[40] Tal y como indica el Comité Europeo de Protección de Datos en su documento: Guidelines 2/2018 on derogations of Article 49 under regulation 2016/679 (25 de mayo de 2018). p. 4.

[41] Manis, M. L. "The processing of personal data in the context of scientific research… *op. cit.* p. 351.

a aquélla y hubiese sido previamente informado de los posibles riesgos[42]. No obstante, la investigación científica y la biomédica, por sus propias características, presentan dificultades a la hora determinar *ex ante* la totalidad de los fines del tratamiento y de recabar los consentimientos de todos los participantes individualmente. Así, la exigencia de un consentimiento explícito para realizar la transferencia sería muy costoso e incluso inabarcable[43], especialmente para grandes proyectos o consorcios supranacionales. Consecuentemente, debe descartarse como una opción generalmente viable, sin perjuicio de que sí podría llegar a emplearse en proyectos más reducidos o de ámbito local.

En segundo lugar, la letra d) del meritado precepto permitiría, excepcionalmente, realizar las transferencias cuando fueran necesarias por razones importantes de interés público. A tales efectos, solo se consideran motivos de interés público aquellos reconocidos en el derecho de la UE o el derecho de los Estados miembros aplicable al responsable del tratamiento[44]. Por tanto, nos hallamos ante una auténtica remisión al derecho interno de los Estados, lo que promueve un marco fragmentado y jurídicamente incierto, pues nada impide que una cuestión que en España pudiera ser considerada como de interés público, en Francia, por ejemplo, no lo fuera. Pese a ello, el tenor del Considerando 112 ha sembrado algunas dudas en tanto en cuanto cita como paradigmas de las razones de interés público, entre otros "intercambios internacionales de datos (…) entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo, en caso de contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte". En todo caso, aunque podría ser todavía discutible, lo cierto es que no constituye el mecanismo idóneo para compartir o transferir datos sensibles de manera permanente en el tiempo, con la inseguridad que de ello se derivaría para los interesados e incluso, desde el punto de vista de la ética de la investigación.

Finalmente, en tercer lugar, el art. 49.1 letra f) legitima las transferencias internacionales que sean necesarias para proteger los intereses vitales del interesado –o de otra persona cuando no esté en condiciones de dar su con-

---

42 A este respecto, el Comité Europeo de Protección de Datos en sus Guidelines 2/2018 *cit.* dispone que son igualmente aplicables las condiciones generales del consentimiento de los arts. 4.11 y 7 del Reglamento pero que, además, deberá añadirse a ello un consentimiento explícito y una información sobre los riesgos.

43 Phillips, M. "International data-sharing norms… *op. cit.* p. 578.

44 Guidelines 2/2018 on derogations of Article 49 under regulation 2016/679, *op. cit.*, p. 10.

sentimiento–. Se trata de un supuesto ya previsto en la DPD cuya aplicación se limita a situaciones de emergencia o urgencia como desastres naturales o humanitarios o incluso para la prestación de asistencia y cuidados médicos transfronterizos en interés de un individuo. Por lo tanto, en todo momento la transferencia debe estar relacionada con el interés del propio individuo, sin que pueda utilizarse dicha excepción "para justificar las transferencias internacionales para desarrollar investigación médica general"[45] como es el caso de la investigación biomédica.

5. Consideraciones finales y propuestas

Por último, procede esgrimir una serie de propuestas que han resultado ser las más convincentes para realizar tratamientos de datos genéticos y de salud y transferencias internacionales de una forma exitosa. Con carácter previo al análisis de los modelos propuestos, es preciso advertir que el mero hecho de aplicar las propias herramientas y principios que introduce el Reglamento puede ayudar considerablemente a reducir *ex ante* los riesgos o las consecuencias negativas de los tratamientos promoviendo, en última instancia, la viabilidad y durabilidad de la propuesta en cuestión. Precisamente, una de las piedras angulares del RGPD es su enfoque claramente preventivo, fomentando medidas tendentes a evitar situaciones de riesgo y dejando atrás una noción puramente reactiva.

Así, por ejemplo, la realización de análisis de riesgos y evaluaciones de impacto –incluso en aquellos supuestos en los que no fuese preceptivo– constituyen un excelente mecanismo para evaluar previamente los riesgos que entrañaría el tratamiento en cuestión o las transferencias de datos genéticos y de salud a otros Estados; pero además, puede servir para identificar las medidas necesarias para cada supuesto concreto de tratamiento y cumplir con las garantías exigibles a los interesados. Como punto negativo encontraríamos el incremento de los costes económicos para grupos de investigación científica cuyos recursos son, habitualmente, limitados[46].

---

[45] Guidelines 2/2018 on derogations of Article 49 under regulation 2016/679, *op. cit.*, pp. 12-13.

[46] Quinn, P. / Quinn, L., "Big genetic data and its big data protection challenges", *Computer Law & Security Review*, Núm. 5, Vol. 34, 2018, p. 1009 [Última consulta: 13 de junio de 2019]. Según los autores, una buena opción sería la de crear un ente o institución de asesoramiento que prestase asistencia para realizar evaluaciones de impacto de manera compartida para una pluralidad de grupos de investigación.

En esta misma línea preventiva podrían citarse otras soluciones mencionadas expresamente por el Reglamento como la designación de un DPO o la observancia del principio de minimización de datos. Finalmente, mas no por ello menos determinante, la aplicación de los principios de protección de datos desde el diseño y por defecto del art. 25 del Reglamento contribuiría al desarrollo de programas y herramientas de gestión y *big data* que *ab initio* incluyesen elevados niveles de protección y seguridad.

5.1. Primera propuesta: un código de conducta para la investigación en salud

Se trata de una de las soluciones especialmente promovidas por el propio Reglamento[47], aunque con carácter previo a la aprobación de la norma ya existían algunos precedentes como, por ejemplo, el ahora cuestionado Código Tipo de Farmaindustria en España[48]. Recientemente, el CEPD ha publicado una Guía en la que proclama que los códigos de conducta son un mecanismo apto para demostrar el cumplimiento efectivo del RGPD (responsabilidad proactiva), para superar las disparidades normativas existentes entre Estados miembros y para adaptar las disposiciones del Reglamento a las operaciones de tratamiento particulares de un sector determinado[49]. Es más, la meritada Guía ofrece como ejemplo de la viabilidad y utilidad de los códigos de conducta su posible respecto a tratamientos de datos de salud con fines de investigación científica, en aras a la uniformización de criterios y la aportación de garantías adecuadas para realizar transferencias internacionales[50].

Al mismo tiempo, un sector de la doctrina ha defendido la aprobación de un Código Internacional para compartir datos genéticos y de salud, basado en la solidaridad y en las declaraciones internacionales de derechos humanos, en

---

47 Art. 40.1: "Los Estados miembros, las autoridades de control, el Comité y la Comisión *promoverán* la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento".

48 Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la farmacovigilancia" (registrado ante la AEPD el 17 de junio de 2009). En la actualidad se encuentra cuestionado debido a que considera expresamente que los datos disociados y los datos codificados no son datos de carácter personal. La realidad actual y la postura del RGPD es bien distinta: se trata de datos relativos a personas físicas identificables y, por ende, sujetos a la normativa.

49 Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 pp. 5 y 9.

50 *Ibídem*, p. 10. En particular, el CEPD establece en este sentido que el uso de códigos de conducta en dicho ámbito puede incluir medidas apropiadas para un tratamiento de datos de salud con fines de investigación de manera uniforme, tales como la aportación de las garantías necesarias del art. 89.1, condiciones para las cesiones o comunicaciones de datos, medidas de seguridad, mecanismos de ejercicio de derechos de los interesados o incluso garantías adecuadas para realizar transferencias internacionales.

tanto factor unificador[51]. Así pues, parece ser una de las vías con más futuro y, de hecho, la elaboración de un Código para el sector de la investigación en salud ya está siendo impulsado a nivel europeo por el BBMRI-ERIC[52].

5.2. Segunda propuesta: cooperación internacional, consorcios y organizaciones

El propio Reglamento insta a la Comisión y a las autoridades de control a fomentar la cooperación internacional con terceros países y organizaciones (art. 50). Por tanto, promover dicha cooperación o, incluso, la creación y el fomento de consorcios u organizaciones de investigación "universales", puede contribuir a la generación de un marco común de intercambio de datos con fines de investigación y, a su vez, superar los escollos para acceder a este tipo de datos en ciertas zonas[53]. Pese a ello, una regulación universal debería enfrentarse a importantes retos jurídicos y éticos –dónde se almacenarían los datos, qué infraestructura sería necesaria para transferirlos internacionalmente, qué mecanismos y bases jurídicas se utilizarían para su recogida etc.–.

Consecuentemente, a día de hoy las principales iniciativas se han articulado en relación a modelos promovidos, en su mayor parte, por organizaciones y consorcios internacionales o paneuropeos como, por ejemplo, *Global Alliance for Genomics and Health*[54], European Open Science Cloud[55], o el *International Cancer Genome Consortium* (ICGC). Cabe aludir expresamente al modelo de acceso controlado propuesto por el ICGC, a través del Data Access Compliance Office (DACO), que ha demostrado ser eficaz y exitoso en la práctica: desde 2008 no ha sufrido ningún incidente de re-identificación ni de uso de datos para finalidades secundarias[56]. Los datos son accesibles

---

[51] Knoppers, B. M. / Harris, J. R. / Dove, E.S. "A human rights approach to an International Code of Conduct for Genomic and Clinical Data Sharing", *Human Genetics,* Núm. 7, Vol. 133, 2014, pp. 897-901. [Última consulta: 20 de junio de 2019].

[52] El BBMRI-ERIC está coordinando la elaboración de un Código de Conducta para la investigación en salud y el desarrollo de nuevos modelos y tratamientos. Más información en: http://www.bbmri-eric.eu/

[53] Badia Martí, A. M. "Los datos genéticos ante el ordenamiento jurídico internacional", *Revista de Derecho y Genoma Humano,* Núm. Extra 1, 2014, p. 304.

[54] Organización internacional que aboga por la creación de políticas y estándares técnicos universales para facilitar un intercambio responsable de datos genéticos y de salud. https://www.ga4gh.org/

[55] Proyecto promovido por la Comisión cuyo objeto es la creación de un *cloud* público y abierto a nivel europeo que sirva para almacenar, buscar y compartir información académica y de investigaciones.

[56] Joly, Y. / Knoppers, B.M. *et. ál.* "Data Sharing in the Post-Genomic World: The Experience of the International Cancer Genome Consortium", *PLoS Computational Biology*, Núm. 7, Vol. 8, 2012, pp. 1-5.

para los investigadores a través de la web del DACO –que realizará un control previo– y tras presentar una solicitud con todas las garantías y responsabilidades. Finalmente, el acceso no se efectúa directamente desde el DACO sino que se consultan las bases de otras instituciones –europeas y canadienses–, que son quienes garantizan que los datos han sido recabados legal y éticamente en origen.

5.3. Tercera propuesta: a falta de hard law, soft law

A lo largo del presente artículo se han puesto de manifiesto ciertas carencias del RGPD y la falta de determinación en la regulación uniforme de determinados aspectos inherentes a los tratamientos con fines de investigación científica. Sin embargo, hay autores que sostienen que, precisamente, esas limitaciones son positivas e incluso, intencionadas, en aras a fomentar el desarrollo de instrumentos *soft-law* y marcos de gobernanza internacional de los datos[57]. Y no se trata, además, de una aproximación disparatada, pues el propio Reglamento consolida las ideas de autorregulación y responsabilidad proactiva, a las que pueden acomodarse perfectamente la aplicación de procedimientos, guías y demás instrumentos de *soft-law.*

A tales efectos, la gobernanza implicaría, en el campo de la investigación en salud, una variedad de enfoques y técnicas destinadas a orientar y monitorizar las actividades de tratamiento sin limitarse únicamente a cumplir con las normas legales ni las reglas del mercado[58]. Por su parte, el *soft-law* supondría acudir a instrumentos no vinculantes como políticas, guías, procedimientos o incluso declaraciones internacionales.

En definitiva, el vertiginoso desarrollo de nuevos métodos de investigación científica unido a los constantes avances tecnológicos convierten a la normas como el RGPD –*hard-law*– en mecanismos, quizás, excesivamente rígidos para adaptarse, por sí solos, al frenético devenir de la sociedad actual. Por tanto, el recurso al *soft-law* podría ser una herramienta válida y exitosa para garantizar una permanente adaptabilidad a los cambios y complementar

---

[57] Mostert, M. / Bredenoord, A. L. / Sloot, B. / Van Delden, J.M. "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", *European Journal of Health Law*, Núm. 1, Vol. 25, 2017, p. 54 [Última consulta: 15 de julio de 2019].

[58] Vayena, E. / Blasimme, A., "Health Research with Big Data: Time for Systemic Oversight", *The Journal of Law, Medicine & Ethics*, Núm. 1, Vol. 46, 2018, pp. 123 [Última consulta: 14 de junio de 2019].

el marco normativo vigente. Esa es, a su vez, su principal debilidad: no pueden sustituir a los instrumentos vinculantes y, por consiguiente, debe existir siempre una base jurídica que justifique el tratamiento y que legitime legalmente las transferencias internacionales de los datos genéticos y de salud, con los problemas ya apuntados al respecto.

6. Bibliografía

Badia Martí, Ana María, "Los datos genéticos ante el ordenamiento jurídico internacional", *Revista de Derecho y Genoma Humano / Law and the Human Genoma Review,* Núm. Extra 1, 2014.

Gonzalo Domenech, J.J., "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados Miembros", *Cuadernos de derecho transnacional*, Núm. 1, Vol. 11, 2019.

Guasch Portas, V. "La computación en nube y las transferencias internacionales de datos en el nuevo Reglamento de la UE", *Revista de Derecho UNED*, Núm. 20, 2017.

Joly, Y. / Knoppers, B.M. *et ál.,* "Data Sharing in the Post-Genomic World: The Experience of the International Cancer Genome Consortium (ICGC) Data Access Compliance Office (DACO)", *PLoS Computational Biology*, Núm. 7, Vol. 8, 2012.

Knoppers, B.M. / Harris, J.R. / Dove, E.S., "A human rights approach to an International Code of Conduct for Genomic and Clinical Data Sharing", *Human Genetics*, Núm. 7, Vol. 133, 2014.

Manis, M. L. "The processing of personal data in the context of scientific research: the new regime under the EU-GDPR", *BioLaw Journal*, Núm. 3, 2017.

Miralles López, R. "Desvinculando datos personales: seudonimización, desidentificación y anonimización. *I+S: Revista de la Sociedad Española de Informática y Salud,* Núm. 122, abril 2017.

Mostert, M. / Bredenoord, A. L. / Van der Sloot, B. / Van Delden, J.M., "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", *European Journal of Health Law*, Núm. 1, Vol. 25, 2017.

Phillips, M. "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)", *Human Genetics,* Núm. 8, Vol. 137, 2018.

Piñar Mañas, J. L. "Las transferencias internacionales en el nuevo reglamento europeo de protección de datos", *Los retos del Estado y la Administración en el siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo*, Vida Fernández, J. (Coord.) / Parejo Alfonso, L.J. (Coord.). Ed. Tirant lo Blanch, Valencia, Vol. 2, 2017.

Quinn, Paul / Quinn, Liam, "Big genetic data and its big data protection challenges", *Computer Law & Security Review*, Núm. 5, Vol. 34, 2018.

SLOKENBERGA, S. "Biobanking between the EU and Third Countries: Can Data Sharing Be Facilitated via Soft Regulatory Tools?", *European Journal of Health Law*, Núm. 5, Vol. 25, 2018.

TAYLOR, M. J. / WALLACE, S.E. / PRICTOR, M., "United Kingdom: transfers of genomic data to third countries", *Human Genetics*, Núm. 8, Vol. 137, 2018.

VAYENA, E. / BLASIMME, A., "Health Research with Big Data: Time for Systemic Oversight". *The Journal of Law, Medicine & Ethics*, ASLME, Núm. 1, Vol. 46, 2018.

7. Normativa citada

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 circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE, L 119/1, 04/05/2016).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE, nº L 281/31, del 23/11/95).

Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 28.I.1981)

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17).

INFORMES / REPORTS

eHealth: los pacientes ante la nueva realidad tecnológica en el ámbito sanitario*

eHealth: patients in the face of the new technological reality in the health field

*Profa. Dra. Virginia Díaz Gorriti***

Profesora en el Departamento de Psicología Social y Metodología de las Ciencias del Comportamiento, Facultad de Psicología en la Universidad del País Vasco UPV/EHU (San Sebastián, España)

*Dra. Rosa Mª Añel Rodríguez****

Médica de Familia en la Unidad de Atención Primaria de Durango, de la OSI Barrualde-Galdakao, en Osakidetza/Servicio Vasco de Salud (Bilbao, España)

Sumario / Summary: 1. Introducción. 2. Hipótesis y objetivos. 3. Resultados. 4. Discusión y Conclusiones. 5. Bibliografía.

---

* Artículo recibido el 20 de septiembre de 2018 y aceptado para su publicación el 9 de junio de 2019.
Conflicto de interés: Las investigadoras declaran no tener ningún conflicto de interés.

** Doctora en Estudios de Ocio y Potencial Humano (2000) por la Universidad de Deusto. Licenciada en Lenguas Aplicadas por la Universidad de Burgos (2003). Licenciada en Ciencias e Historia de la Música por la University of London, Goldsmiths´ College (1994). Licenciada en Filosofía por la Universidad de Deusto (1990).

*** Licenciada en Medicina y Cirugía General por la Universidad del País Vasco (1997), Especialista en Medicina Familiar y Comunitaria (2001), Máster en Participación y Desarrollo Comunitario (2018).
Ha sido referente de Seguridad del Paciente desde el año 2010 y forma parte del Equipo corporativo de Coordinación de Programas de Salud Pública y Seguridad del Paciente de Osakidetza desde el año 2017.

Resumen / Abstract: En la actualidad la tecnología, su comprensión y aplicabilidad en muchos escenarios de la vida diaria de las personas, así como la producción de transformaciones radicales en cuanto a la irrupción y asentamiento de nuevos modelos socio sanitarios, resulta un tema de profunda complejidad. Por ello, para entender dichas transformaciones y como son percibidas por la ciudadanía, resulta necesario incorporar sus voces, discursos y narrativas sobre *eHealth*.

Nowadays, technology, its understanding and applicability in many daily arenas, as well as the production of radical transformations in terms of the emergence and establishment of new social and health models, is a matter of deep complexity. Therefore, to understand these transformations and how they are perceived by citizens, it is necessary to incorporate their voices, discourse and narratives about eHealth.

Palabras clave / Keywords:

eHealth / Discursos / Agencia del paciente / Sentido común.

eHealth / Discourses / Patient agency / Common sense.

1. Introducción

El gran reto que supone en la actualidad la tecnología, su aplicación y comprensión en la vida diaria de las personas, así como la producción de transformaciones paradigmáticas en cuanto a emergencia y asentamiento de nuevos modelos socio sanitarios para dar cobertura y solución a los problemas que afronta el gasto público en sanidad despunta como crucial y merecedor de profundos abordajes. Por ello, y para entender dichas transformaciones, resulta necesario incorporar voces, agencias y narrativas del sentido común en los discursos de este nuevo orden disciplinar que es la *eHealth*.[1]

Dado que el nuevo contexto tecnosocial cambia constante e inexorablemente[2] surgen nuevas preguntas con soluciones que remiten al nuevo campo de actuación de *eHealth*[3]. Además, cabe reseñar que, entre las demandas sociales actuales, la mayoría de usuarias y usuarios de la institución sanitaria

[1] Black, Ashly D. *et ál.,* "The impact of eHealth on the quality and safety of health care: a systematic overview", *PLoS medicine*, Núm. 1, Vol. 8, 2011, p. e1000387.

[2] Ross, Jamie *et ál,* "Exploring the challenges of implementing e-health: a protocol for an update of a systematic review of reviews", *BMJ open*, Núm. 4, Vol. 5, 2015, p. e006773.

[3] Dinesen, Birthe, *et ál.,* "Personalized telehealth in the future: a global research agenda", *Journal of medical Internet research*, Núm. 3, Vol. 18, 2016.

muestran un gran interés por la información [4], la seguridad y la privacidad, así como por su distribución[5].

Colateralmente, la ubicuidad de los dispositivos móviles se halla presente en todas las escenas de la vida de la ciudadanía y por ello, su uso y normalización como vía comunicativa en la institución sanitaria, *eHealth*[6], puede suponer la disminución de la percepción del riesgo sistémico y la obtención casi instantánea de data fundamental. Efectivamente los teléfonos móviles, sus características y potencialidades han sido el centro y eje de atención de la mayoría de las instituciones[7] y por ello la realidad social en la que vivimos se enfrenta a nuevos desafíos: educativos, sanitarios, administrativos[8]. El WhatsApp, en este ámbito de la salud[9], puede ser una herramienta eficaz para mejorar la calidad de la asistencia, además de erigirse como un nuevo horizonte epistemológico de la comunicación en salud. En el escenario web se posibilita un universo del discurso más democrático, amplio, plástico, personal y contextual[10] permitiendo establecer una comunicación directa con las audiencias específicas, adaptándose a su contexto a través de la personalización de la información que permite la web. El *copyright* o *derecho de copia* despunta como gran incógnita y blinda el derecho exclusivo legal al usuario para ejercer el control sobre la copia generada y todo tipo de explotación de lo generado o creado durante un período específico de tiempo. Desde la virtualidad, esos derechos de copia deben estar sometidos a limitaciones y

---

4 Parascandola, Mark / Hawkins, Jennifer Susan / Danis, Marion, "Patient autonomy and the challenge of clinical uncertainty", *Kennedy Institute of Ethics Journal*, Núm. 3, Vol. 12, 2002, pp. 245-264.

5 Benlloch Domènech, Cristina / Sarrión Esteve, Joaquín, "eSalud-administración sanitaria digital", *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Ed. Thomson Reuters Aranzadi, Cizur Menor, España, 2018, pp. 499-529.

6 Sclafani, Joseph / Tirrell, Timothy F. / Franko, Orrin I., "Mobile tablet use among academic physicians and trainees", *Journal of medical systems*, Núm. 1, Vol. 37, 2013, p. 9903.

7 Andrawis, John P. / Muzykewicz, David A. / Franko, Orrin I., "Mobile device trends in orthopedic surgery: rapid change and future implications", *Orthopedics,* Núm. 1, Vol. 39, 2016, p. e51-e56. ttp://www.ehu.eus/ojs/index.php/papelesCEIC/index

8 Tindell, Deborah R. / Bohlander, Robert W., "The use and abuse of cell phones and text messaging in the classroom: A survey of college students", *College Teaching*, 2012, Núm. 1, Vol. 60, 2012, pp. 1-9.

9 Nardo, Bruno *et ál*, "Optimizing patient surgical management using WhatsApp application in the Italian healthcare system", *Telemedicine and e-Health*, Núm. 9, Vol. 22, 2016, pp. 718-725.

10 Yeates, Karen *et ál,* "The Effectiveness of Text Messaging for Detection and Management of Hypertension in Indigenous People in Canada: Protocol for a Randomized Controlled Trial", *JMIR research protocols*, Núm. 12, Vol. 6, 2017.

excepciones. Cualquier otro uso requerirá la licencia o solicitud de permiso de autoría para permitir o autorizar sus derechos exclusivos a terceros. De esa forma la participación ciudadana, que contrae agencia, comunica socialmente al sentir de los pacientes siendo este derecho de copia el patrón de habla y acción, en el que se interrelacionan de manera tal y en el que se verifica el cumplimiento de las expectativas grupales[11].

En efecto, se puede afirmar sin ningún tipo de dudas que vivimos en la era de la información y que toda ella deja su huella. La infinita meta-generación de datos y tanto su publicación como almacenaje pueden ser o convertirse en una cuestión de suma importancia para un ámbito tan delicado y frágil en su tratamiento como puede ser el campo de la salud. El problema de la interpretación de este término es central y causa problemas. Incluso puede convertirse un problema en sí mismo. Como cuestión lógica, conocer qué es el copyright y cuál debe ser su función, puede ser crucial para la determinación clara de su ser y alcance. Para muchos profesionales su significado parece ser claro y distinto frente a otros que lo utilizan en otros contextos y con diferente matización[12]. Desde el socioconstruccionismo, como aproximación discursiva y metateoría explicativa de los hechos sociales del mundo, podríamos aproximarnos a entender que es lo que entiende y conoce la población por este constructo de *eHealth* sociosanitario, por un lado, y de la generación de metadatos, por otro, e intentar estudiar, a su vez, la relación entre esa realidad postmoderna tecnológica (*eHealth*) y las posiciones de los sujetos (en tanto que propietarios de datos) a la hora de acercarse a esa nueva realidad sociosanitaria[13]. Todavía para la gran mayoría la población usuaria de la sanidad pública su significación y entendimiento no está claro y por ello debe pulirse aquello a lo que remite y cuál puede ser su utilidad[14]. Además, dentro de las propias lógicas sanitarias emerge el problema de la interpretación y exegesis de este término, resultando central y causante de ulteriores problemáticas. Y si lo anterior resultaba dudoso, nuevos retos salen a la arena epistemológica, dada la prolífica generación

---

[11] Wagner, Wolfgang / Hayes, Nicky / Flores, Fátima, "El discurso de lo cotidiano y el sentido común. *La teoría de las representaciones sociales*", *Anthropos*, Barcelona*,* España*,* 2011.

[12] Beuscart-Zephir, M.C. *et ál,* "Cognitive evaluation: how to assess the usability of information technology in healthcare", *Computer methods and programs in biomedicine*, Núms. 1-2, Vol. 54, 1997, pp. 19-28.

[13] Shotter, John *et ál. Realidades conversacionales: la construcción de la vida a través del lenguaje*, 2001.

[14] Showell, Chris / Nohr, Christian, "How should we define eHealth, and does the definition matter?". *Quality of life through quality of information*, Vol. 180, 2012, pp. 881-884.

de datos: que se hace o debe hacer con ellos. Cuáles son los proteicos usos que de ellos se pueden hacer es un nuevo horizonte epistemológico de posibilidades infinitas que se le abren al paradigma *eHealth*[15].

En cualquier caso, lo que desea y demanda la población usuaria en general, y los pacientes en particular, es información pertinente y de fácil y libre acceso, que hasta ahora le ha sido denegada. Desde el sentir del sujeto paciente, el devenir de la medicina y del conocimiento médico se le ha ocultado ésta, tras una metanarrativa oscura, difícil e incomprensible, ofrecida como una única moneda de cambio a la población lega. Este tipo de información no pertenece a las demandas que solicitan los pacientes con agencia que acuden al centro de atención primaria u hospitalaria. Lo que esas personas desde sus posiciones de sujeto activo y participante solicitan –y es aquí donde entra en juego el papel de *eHealth*– es que sean tenidas en cuenta en su paradójica situación de paciente-agente de su condición, dolencia, enfermedad, etc. En la obsoleta relación del pasado monológica, tensa y compleja pueda ahora, dado este nuevo horizonte tecnológico *eHealth*, tal vez, el sujeto paciente encuentra que puede convertirse en dialógica, distensa y multifacética. Como ya se ha avanzado, para el construccionismo discursivo[16] los eventos sociales, los sucesos del mundo son construidos mediante argumentos y representaciones. Ellos son los que dotan de sentido a la realidad social, ya que lo que nos rodea no son propiedades o fuerzas externas sino el relato de esos fenómenos que nos suceden social y culturalmente. Lo acontecido solo existe y persiste si se insiste en su relato, si no carece de principio de verificación por lo que no podemos confirmar su existencia. Los límites del mundo son los límites del lenguaje, y conocer, construir y entender lo que es el nuevo paradigma sanitario de *eHealth*, es un proceso en la que se ve envuelta la realidad tanto social, como sanitaria.

2. Hipótesis y objetivos

Para entender el advenimiento de una nueva arena sociosanitaria como es *eHealth* a la que nos arroja la tecnología, en la que la solidez de los fundamentos teóricos y ontológicos del pasado ya no parecen existir, y para estudiar la conformación en curso de nuevos socioconstructos como el de *eHealth*, que nos puedan servir para la comprensión o incomprensión del

[15] Oh, Hans *et ál.* "What is eHealth (3): a systematic review of published definitions", *Journal of medical Internet research*, Núm. 1, Vol. 7, 2005.

[16] Wetherell, Margaret *et ál, Discourse as data: A guide for analysis*, Sage, Londres, Reino Unido, 2001.

mundo y escenario sanitario tanto tradicional como virtual, se plantearon las siguientes hipótesis:

1) Un amplio porcentaje de la ciudadanía desconoce qué es el nuevo paradigma sociosanitario *eHealth* y lo que comporta.

2) La población usuaria de los servicios sanitarios, tanto en versión *eHealth* como en el modelo tradicional, demanda información para desarrollar su agencia participativa.

3) La información siempre es necesaria para la participación del paciente durante la asistencia.

3. Metodología

La función que cumple una investigación cualitativa es la de proporcionar una metodología que permita comprender el complejo mundo de la experiencia vivida desde el punto de vista de las personas que la viven. Por ello se estudió como las personas participantes comunican y dan sentido a lo que ellas entienden por *eHealth* y autoría de datos generados (*copyrights*) mediante el análisis del discurso de las respuestas dadas. Para entender y analizar en los discursos de la población usuaria el constructo sanitario *eHealth*, y su perimetraje de entendimiento, se llevó a cabo una encuesta que constaba de 9 preguntas sencillas y de fácil respuesta sobre este neoconstructo o paradigma sanitario. A partir de las respuestas comunicadas lo que se pretendía analizar es cómo se construye el ideologema *eHealth* y si la población entiende lo que puede suponer su implementación que con el paso del tiempo presuntamente podría desplazar al modelo tradicional más centrado en los profesionales. El propósito era contribuir a un examen crítico de lo que supone el socioconstructo todavía en proceso de factura de *eHealth* desde un enfoque discursivo, poniendo de manifiesto la construcción, edificación y refuerzo de las representaciones sobre este nuevo constructo, ideologema sociocultural, sus prácticas sociales y las relaciones que se establecen y pueden a su vez generar. Dicho envío comenzó desde los contactos personales y profesionales de las investigadoras. La población participante, a su vez, empezó a pasar dicho enlace a otros contactos profesionales, sociales y redes. De esta forma, se consiguió una participación plural y heterogénea. La muestra buscaba ser lo más variada y abierta posible para obtener información útil que ayudara a desvelar los aspectos ocultos en las percepciones regulares, y además capturar los temas centrales y/o las

principales características que tipifican una realidad humana relativamente estable.

4. Resultados

Cuando se analizan los discursos de las personas participantes se obtiene una muestra de los principios de jerarquización del conocimiento que sufren las personas a la hora de expresarse de darse a entender. Fueron muchas las personas que comunicaron que desconocían lo que era el nuevo constructo de *eHealth*, de las 65 que contestaron a esta encuesta. Así, del total de personas participantes, 31 comunicaron que desconocían qué es el *eHealth* frente a 34 que si lo conocían. Del total de participantes, 56 tenían estudios universitarios y también esos 56 conocían que al acudir a un centro sanitario se generan nuevos metadatos. Cuando se les preguntó a quién pertenecían esos datos, fueron esos 56 participantes quienes contestaron que a la propia persona (como paciente o usuaria). En la pregunta que hacía referencia a si le gustaría disponer de esos datos, 59 ratificaron que les gustaría disponer de ellos como si de un boletín libre y abierto se tratara y que les llegara. Con la pregunta de si esos datos deberían utilizarse con otros propósitos es cuando más se observa que comienzan a polarizarse las posiciones de los sujetos. En todo momento se observó que las respuestas fueron consolidadas y apenas existía polarización grupal. Únicamente emerge el estado bifronte en el caso de la pregunta sobre si conocen qué es *eHealth*. En esta pregunta el *footing* del sujeto se halla claramente confrontado. Unos hablan como voces expertas, que saben lo que es y se presentan como conocedores y voces que articulan posiciones de poder (o desarrollo de su capacidad de agencia), sobre aquellos que contestan desconocerlo. También son 56 los participantes que refieren situarse en contra de un mal uso o abuso de usos datos. Se trata de participantes tipo que se expresan de la siguiente manera: "Si, para prevenir enfermedades y ofrecer una mejor atención médica" y "Sí, para fines de investigación".

De nuevo comunican en sus discursos que: "Depende del objetivo" y "Solo si se posee el consentimiento del paciente".

En esa muestra de la realidad bipolar que se construye en torno a *eHealth* se puede evidenciar que hay siempre dos tipos de poblaciones: los que ejercen el poder cognoscitivo (expertos y conocedores) y los que lo carecen, los subordinados (ignorantes y desconocedores). Son 10 los participantes que ejercen el conocimiento a la hora de contestar dando y comunicando lo

que ellos, voces expertas, piensan que es *eHealth*, frente a aquella otra parte de la población silente, 31 personas, que parece no saber o no querer dar a conocer aquello que entiende por ese neoconstructo de *eHealth*. Cuando a estos participantes se le preguntó por *eHealth* utilizaban el elemento del sentido común construyendo un entendimiento social compartido y dando a entender mediante el lenguaje que era para ellos el ideologema *eHealth*. Todas esas voces construían una idea de la versión social de ese nuevo escenario *eHealth*. Algunos mostraron el dilema del interés (*dilemma of stake*) sobre lo que decían o comunicaban y, no queriendo parecer implicados o desconocedores, producían una versión que contrarrestaba que tuvieran algún interés o claro desconocimiento, no dando una versión acertada.

Participante 1 "No sé. Lo siento, es un término desconocido. Seguramente conozca la idea, pero no la etiqueta eHealth) que la define".

Participante 2 "No lo sé. No concibo ningún otro propósito para su uso. Sobre todo, si son datos sobre salud. Considero que se pueden utilizar siempre y cuando sea informada debidamente sobre su uso".

Se observó en las respuestas como los participantes construían una acepción factual de la definición, su entendimiento del estado de las cosas, y al mismo tiempo edificaban un *self* positivo de sí mismos, reconstruyendo un estatus de perceptor fiable y racional. Su posición como sujeto remitía a la propia experiencia, evaluando los diferentes discursos de los sujetos que conformaban la muestra. Claramente optaron por una posición de encuestado frente a la de la investigadora (tal vez con menos ejercicio de poder ya que la figura del encuestador es la de manejar los datos y subordinar aspectos de éstos, de acuerdo a lo que se quiera analizar y/o teorizar). Además, se quedó mostrado como su posición podía variar dependiendo de si comunicaba como usuario, como cuidador o como paciente. Estos comunicantes cambiaban y manejaban el discurso para alcanzar en él un mayor manejo del control y poder. Las personas participantes de la encuesta quisieron a lo largo de ella mantener un *self*, una autoimagen positiva asegurándose que sus creencias y valores fueran los compartidos. Por el contrario, los participantes del segmento del silencio, representaron el temor a comunicar o a desconocer o fallar y por ello protegieron su *self* (desconocedor) con los espacios en blanco y silencios manifiestos. Estas no respuestas o espacios en blanco dicen mucho sin utilizar las palabras del lenguaje natural. Son participantes que se sintieron sin poder para hacer efable su mundo comunicativo, sin agencia. Se vieron arrojados a un contexto situacional estresante al no saber comunicar. Sus posiciones eran las de no saber o no querer contestar

por temor a fallar, por el riesgo que percibían a expresar sus pareceres u opiniones, tal vez erróneamente. Este silencio, lo sintieron y lo percibieron como realidad, como algo normalizado. Esta polarización contrastó con las voces expertas que contestaron, que dieron acepciones más certeras de la realidad, que se enfrentaban polarmente a la del silencio de las restantes. Las posiciones del sujeto se movieron entre ostentar poder epistemológico y evidenciar su ausencia de poder para manejar la situación constante. Así pues, se ha se subrayar que el análisis del discurso enfatizó las relaciones y las creencias sobre la realidad *eHealth* y cómo era usada y comunicada ésta por las personas participantes. En los discursos se evidenció la diferencia entre el uso lingüístico y la práctica social que vive en decurso sanitario: que para unos es un escenario de pura abstracción intelectual (los participantes que aportan sus opiniones libremente) y para otros un ámbito de desconocimiento, silencios y tensiones (participantes que no contestan).

Desde el análisis del discurso se descubrió también que existe un amplio bastión de agencia y posición del sujeto a la hora de corroborar en la afirmación de la necesidad de conocer esos datos generados por los pacientes. Conocer que esos datos pueden ser utilizados para evaluar y conocer las actitudes y comportamientos de un determinado segmento poblacional, imprime un gran riesgo y por ello, lo consideran de gran pertinencia ser informado de ellos y tenidos en cuenta sobre las necesidades sanitarias y sociales futuras. En sus discursos, además, queda implicado otro de los dilemas que se pueden traer a colación: *el dilema del montón*. ¿Cuántos granos son un montón de arena? ¿Cuántos datos son necesarios para ser un *Bigdata*?

5. Discusión y Conclusiones

Para el presente artículo la información fue investigada utilizado el análisis de los discursos de los participantes en la encuesta. El objetivo inicial era conocer como las y los usuarios de la sanidad pública comunican sus actitudes, creencias y valores sobre el nuevo sociocontructo sanitario *eHealth.* Anticipábamos además que todavía este constructo se halla en desarrollo y no es plenamente conocido por la toda la ciudadanía. Este dato se confirmó ya que muchos de los participantes desconocían la existencia del socioconstructo *eHealth* y de la metageneración de datos que de ella puedan surgir. De esta manera se confirma que la sanidad actual mantiene todavía su relación de corte tutelar y lo sanitario se coloca como superior frente al sujeto usuario. Lo que parece poder deducirse de los datos es que la totalidad de las personas participantes consideran deseable la aceptación del modelo de

la salud electrónica basada, y que de ella recibieran información constante para conocer lo que concierne al ámbito campo de su salud personal. El tema del conocimiento como ejercicio de poder queda implicado en este análisis. Lo que nos ha interesado averiguar colateralmente a su vez es cómo se reproducen, construyen y negocian esas relaciones de poder (en cuento conocimiento-desconocimiento). Por ello nos preguntamos: si *eHealth* es una realidad en el trasunto sanitario, ¿no es inquietante que todavía mucha parte de la ciudadanía, muchos usuarios con altos conocimientos y capacitaciones, desconoce su existencia y los ulteriores usos que de ella puedan surgir, unos útiles y ventajosos y otros tal vez taimados y peligrosos según el arbitraje que se haga de ellos?

Se constata, además, como el conocimiento sigue constituyendo un dispositivo de poder. Lo que se ha concluido en esta investigación es que la medicina aun lleva el control de la agenda pero que la ciudadanía en sus respuestas intenta llevar a cabo intentos de redefinición de las identidades y de las relaciones sociales implicadas. Las implicaturas halladas en las respuestas es el desafío a la dominación. Lo comunicado por los participantes se consideran prácticas discursivas "creativas" que contribuyen a los cambios sociales: que pacientes y usuarios quieren conocer y acceder a esos datos que se generan. Así pues, en esta investigación ha quedado constancia de que al construir desde el lenguaje nuestra realidad social quedamos inevitablemente investidos en determinadas posiciones de sujeto que nos sirve para analizar la relación entre el *self,* la identidad y los discursos y cómo tanto el *self* como nuestra identidad como usuarios, pacientes, cuidadores, hombres, mujeres, padres, madres, extranjeros, indocumentados, se encuentran constantemente entrelazadas.

Nuevas preguntas surgen en este nuevo escenario de fusión de horizontes, tales como: ¿Resulta necesario establecer nuevos patrones relacionales en *eHeath* entre el paciente y la sanidad?, ¿Se han de propiciar nuevos espacios de actuación individual, social y comunitaria que posibilite avanzar hacia la toma de decisiones sanitarias y personales?, ¿Es/debe ser el paciente propietario de los data generados cuando acude a consulta?¿Desde la cultura de *eHealth* se reconocerá la figura del/la paciente autónomo, independiente y gestor de su salud a nivel individual, y protagonista y colaborador constructor de un sanidad mejor y con futuro, a nivel social y comunitario?

Se ha de tener siempre presente que actualmente el escenario de actuación de *eHealth* y sus proteicas manifestaciones esta poco regulado y que

ella en sí misma, si su implementación resulta defectuosa, puede ser capaz de causar ulteriores daños a pacientes y usuarios.

Resulta necesario realizar más investigaciones sobre la aplicabilidad del WhatsApp en relación con la cultura de la participación del paciente, ya que serviría para que esta se convirtiera en una herramienta común y aceptada por la comunidad y las personas usuarias de la sanidad para identificar escenarios de riesgo, deficiencias o áreas de mejora.

A su vez, en los discursos distintas implicaturas quedan constatadas. Desde el punto de vista individual: ¿Cómo se relacionan las descripciones de *eHealth* con las descripciones de las personas y sus estados psicológicos? ¿Cómo arregla la persona que habla o escribe la posibilidad de que su versión de los hechos se considere "interesada" o parcial, o pueda ser descartada o debilitada por el hecho de evocar prejuicios, motivos ocultos, implicaciones emocionales, etc.? Desde el punto de vista socio comunitario: ¿Podrán ser comercializados los *Bigdata* generados con fines diversos o perversos? ¿Quién/qué llevará a cabo la gestión o control de esos data? ¿Dónde se guardarán esos data? Algunas de estas reflexiones resultan inquietantes y por ello nos inspiran hacia nuevos estudios y futuros análisis.

5. Bibliografía

Andrawis, John P. / Muzykewicz, David A. / Franko, Orrin I., "Mobile device trends in orthopedic surgery: rapid change and future implications", *Orthopedics*, Núm. 1, Vol. 39, 2016.

Benlloch Domènech, Cristina / Sarrión Esteve, Joaquín, "eSalud-administración sanitaria digital", *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Ed. Thomson Reuters Aranzadi, Cizur Menor, España, 2018.

Beuscart-Zephir, M.C. *et ál,* "Cognitive evaluation: how to assess the usability of information technology in healthcare", *Computer methods and programs in biomedicine*, Núms. 1-2, Vol. 54, 1997.

Black, Ashly D. *et ál.,* "The impact of eHealth on the quality and safety of health care: a systematic overview", *PLoS medicine*, Núm. 1, Vol. 8, 2011.

Dinesen, Birthe *et ál.*, "Personalized telehealth in the future: a global research agenda", *Journal of medical Internet research*, Núm. 3, Vol. 18, 2016.

Nardo, Bruno, *et ál*, "Optimizing patient surgical management using WhatsApp application in the Italian healthcare system", *Telemedicine and e-Health*, Núm. 9, Vol. 22, 2016.

Oh, Hans, *et ál.,* "What is eHealth (3): a systematic review of published definitions", *Journal of medical Internet research*, Núm. 1, Vol. 7, 2005.

PARASCANDOLA, Mark / HAWKINS, Jennifer Susan / DANIS, Marion, "Patient autonomy and the challenge of clinical uncertainty", *Kennedy Institute of Ethics Journal*, Núm. 3, Vol. 12, 2002.

ROSS, Jamie *et ál.,* "Exploring the challenges of implementing e-health: a protocol for an update of a systematic review of reviews", *BMJ open*, Núm. 4, Vol. 5, 2015.

SCLAFANI, Joseph / TIRRELL, Timothy F. / FRANKO, Orrin I., "Mobile tablet use among academic physicians and trainees", *Journal of medical systems*, Núm. 1, Vol. 37, 2013.

SHOTTER, John *et ál., Realidades conversacionales: la construcción de la vida a través del lenguaje*, 2001.

SHOWELL, Chris / NOHR, Christian, "How should we define eHealth, and does the definition matter? ", *Quality of life through quality of information*, Vol. 180, 2012.

TINDELL, Deborah R. / BOHLANDER, Robert W., "The use and abuse of cell phones and text messaging in the classroom: A survey of college students", *College Teaching*, 2012, Núm. 1, Vol. 60, 2012.

WAGNER, Wolfgang / HAYES, Nicky / FLORES, Fátima, "El discurso de lo cotidiano y el sentido común. *La teoría de las representaciones sociales", Anthropos*, Barcelona*,* España*,* 2011.

WETHERELL, Margaret *et ál., Discourse as data: A guide for analysis*, Sage, Londres, Reino Unido, 2001.

YEATES, Karen *et ál,* "The Effectiveness of Text Messaging for Detection and Management of Hypertension in Indigenous People in Canada: Protocol for a Randomized Controlled Trial", *JMIR research protocols*, Núm. 12, Vol. 6, 2017.

IntimidAPP: Los problemas del tratamiento de datos biosanitarios en *wearables* y *apps* para móviles*

Privacy: The problems of biosanitary data processing in wearables and apps for mobiles

*Alberto Hidalgo Cerezo***

Abogado

Doctorando en Derecho y Ciencias Sociales por la Universidad Nacional de Educación a Distancia (Madrid, España)

Sumario / Summary: 1. Introducción. 2. Los datos biosanitarios en línea: sensibilidad, especial consideración y alto valor. 3. Los wearables, el granjeo constante de datos y monitorización de actividades. ejemplos reales a la luz de dispositivos en el mercado. 4. El potencial invasivo a través de casos reales. Obtención del consentimiento estratificado o por capas y su viabilidad tecnológica. 5. Conclusiones. 6. Bibliografía.

Resumen / Abstract: La entrada en vigor del Reglamento General de Protección de Datos el pasado 28 de mayo alcanzó cierta notoriedad entre la ciudadanía, normalmente desapegada de todo celo sobre sus datos de carácter personal. Ello se debió a la necesidad por parte de diferentes aplicaciones y servicios digitales de recabar de nuevo el consentimiento, para encontrarse acorde con los estándares del RGPD, y poder seguir tratando los datos de los usuarios. Sin embargo, pasado el revuelo inicial, y tras volver a aceptar todo tipo de cláusulas y condiciones sin haberlas leído detenidamente, encontramos que muchas aplicaciones y servicios recaban y tratan multitud de datos sanitarios y biométricos, cuyo tratamiento está prohibido por

* Artículo recibido el 15 de octubre de 2018 y aceptado para publicación el 2 de septiembre de 2019.

** Dirección de correo electrónico: a.hidalgo@icam.es. Este trabajo es uno de los resultados obtenidos durante la estancia de investigación entre junio y octubre de 2018 en el Centro de Investigação Jurídico-Económica de la Universidad de Oporto. Quisiera dar mi agradecimiento a la profesora María Raquel Guimarães por su apoyo constante y sus generosos consejos.

defecto al tratarse de datos especialmente sensibles. Por ello, se encuentran sujetos a la obtención del preceptivo consentimiento "expreso y por escrito" que exige el art. 9.2.a) del RGPD para este tipo de datos. No hablamos solo de las "imágenes faciales o datos dactiloscópicos" con los que el art. 4.14 ejemplifica los datos biométricos, sino también de informaciones mucho más elaboradas como las que se obtienen a través de pulseras deportivas, básculas inteligentes, y otros datos altamente sensibles por sí mismos. La posibilidad de combinación de diversos datos en clave Big Data, y el riesgo de creación de perfiles en base a ellos, constituye una seria amenaza que afecta claramente al derecho fundamental a la intimidad y a la protección de datos de carácter personal.

General Data Protection Regulation became enforceable on last May 28th and reached a certain notoriety among citizens, often inattentive over their personal data. This was due to the need of different digital applications and services to obtain users' consent again in accordance with the new standards set by the GDPR, in order to be able to keep treating their data adequately. However, after the initial fuss, and after accepting all kinds of clauses and conditions without having read them carefully, we find that many applications and services collect and process a wide variety of health and biometric data, whose treatment is forbidden by default because of their especially sensitive nature. For this reason, treatment of these data is subject to obtaining the mandatory "express and written" consent required by art. 9.2.a) of the RGPD for this kind of data. We do not speak only of the "facial images or dactyloscopic data" exemplified in art. 4.14 about biometric data, but also of a much more elaborate information, such as those obtained through sports wristbands, smart scales, and other highly sensitive data. The possibility of combining diverse data with the power of Big Data, and the risk of creating profiles based on them, constitutes a serious threat that clearly affects the fundamental right to privacy and to the protection of personal data.

Palabras clave / Keywords:

RGPD / Protección de datos / Tratamiento de datos personales / Datos relativos a la salud / *Wearables* / Aplicaciones / Teléfonos inteligentes / Big Data / Internet de las cosas (IoT) / Consentimiento / Privacidad / Tratamiento.

GDPR / Data protection / Processing of personal data / Data concerning health / Wearables / APPs / Smartphones / Big Data / Internet of Things (IoT) / Consent / Privacy / Processing.

1. Introducción

La autodeterminación informativa responde a un principio esencial: no existe verdadera libertad si el individuo se siente observado en su decisión, o si, en base a su perfil, pueden preverse sus siguientes movimientos, lo que permite a otros agentes alterar y adaptar sus comportamientos para acomodarse a aquellos. Será, en todo caso, una libertad ilusoria, un pequeño "show de Truman" que puede apreciarse en multitud de pequeñas decisiones a lo largo de todo el día, en la medida en que las opciones que se presentan al individuo resultan moldeadas a sus preferencias. Nótese que, en el medio

digital, es frecuente encontrarse con elementos adaptados a nuestro perfil. Resulta obvio que tales elecciones adaptadas no se encuentran encaminadas a ayudar al sujeto, sino a maximizar los beneficios –finalidad plenamente legítima y que no se discute en modo alguno– de las compañías que explotan los datos como fuente de riqueza[1]. La afectación abarca muchas otras situaciones que, en el pasado, y con menos información de la que hoy día generamos gracias a todo tipo de dispositivos, ya han dado lugar a situaciones indeseables (que expondremos), invadiendo otros derechos fundamentales como el derecho a la no discriminación, el libre desarrollo de la personalidad, y en general, a la "facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida", como ya vaticinó hace 35 años una resolución que parece adelantada a su tiempo: la Sentencia BvR 209/83 de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán.

Los ejemplos están a la vista en nuestra vida cotidiana. Si buscas un vuelo, aunque no fuese para ti, comenzará a aparecerte publicidad de compañías aéreas[2]. Si eres mujer, alrededor de la treintena, es muy posible que estés familiarizada con anuncios de tests de embarazo[3]. Hasta los botones de "me gusta" insertos en páginas webs de terceros han servido para realizar seguimientos mientras navegamos[4], incluso sin ser usuarios de Facebook[5], por no mencionar la gravedad del reciente caso Cambridge Analytica[6] –cuyo

---

1 Vázquez De Castro, Eduardo, "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías* Núm. 46, 2018 (sección Estudios Jurídicos), BIB 2018\7467.

2 Diario El País, edición de 15 de octubre de 2015: "*Retargeting*: *¿Por qué ese anuncio de Internet no deja de perseguirme?":* https://elpais.com/tecnologia/2015/10/13/actualidad/1444761762_059471.html [Última consulta: 29 de julio de 2018].

3 Diario El Mundo, edición de 24 de noviembre de 2016: "Mujer, en torno a los 30, europea: ¿Por qué te acosa Clearblue en YouTube?": http://www.elmundo.es/f5/comparte/2016/11/24/58356f26e2704e59368b4640.html [Última consulta: 29 de julio de 2018].

4 Diario The Guardian, edición de 31 de marzo de 2015: "Facebook 'tracks all visitors, breaching EU law'": https://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report [Última consulta: 30 de julio de 2018].

5 Diario El Mundo, edición de 12 de junio de 2018: "Zuckerberg lo reconoce: Facebook recopila datos hasta de quien no tiene cuenta": http://www.elmundo.es/tecnologia/2018/06/12/5b1fbbb822601dbf488b4622.html [Última consulta: 30 de julio de 2018].

6 La investigación fue llevada a cabo por los diarios The Guardian (https://www.theguardian.com/news/series/cambridge-analytica-files) y The New York Times (https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html). En español, https://www.bbc.com/mundo/media-43655680 [Últimas consultas: 30 de julio de 2018].

sugerente eslogan es: "data drives all that we do"–[7]. Lo que aquí se trata de significar es que la explotación de nuestros datos excede, con mucho, de la punta del iceberg que es la proclamación del derecho a la protección de datos de carácter personal, tratándose de un fenómeno muchísimo más amplio y complejo. En otras palabras: no podemos caer en la ingenuidad de que la información que generamos se mantiene en nuestra esfera privada, como si de un compartimento estanco se tratara.

No es necesario mirar mucho más allá para apreciar que existe una afectación evidente a la libertad desde todos los ángulos (intimidad personal y familiar, autodeterminación informativa, libre desarrollo de la personalidad, etc.[8]). Como ya se ha dicho con anterioridad: *"Aparece ante todo amenazada por* el hecho de que los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y documentos compilados manualmente; antes bien, hoy día, gracias a la ayuda de la elaboración automática de datos, la información individual sobre circunstancias personales u objetivas de una persona determinada o en su caso, determinable, […] son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquier que sea la distancia. Es más, esa información puede –especialmente con el montaje de sistemas integrados de información– refundirse con otras colecciones de datos en un perfil de

[7] Web oficial de Cambridge Analytica: https://cambridgeanalytica.org/ [Última consulta: 30 de julio de 2018].

[8] Luzak, Joasia, "Is All Fair in War Against Unhealthy and Unsustainable Lifestyles? The Right to Privacy vs. Modern Technology in Consumer Contracts", *The Constitutional Dimension of Contract Law: A comparative perspective*, Siliquini-Cinelli, Luca / Hutchison, Andrew (Eds.), Springer International Publishing, Cham, Suiza, 2017, pp. 39-59. En su página 41: "Regrettably, policy measures that are effective in combating unhealthy consumer choices may, nonetheless, simultaneously, infringe consumer autonomy and privacy". Asimismo, en las páginas 41 y 42: "The right to privacy may become a victim of the fight for better consumer lifestyles, when policymakers and traders support the use of modern technology, without introducing a strict regulation thereof. (…) Modern technology allows retailers to label their products electronically using so-called RFID (radio-frequency identification) tags. That is to say, consumer products contain a smart chip that allows traders to track them. On the one hand, this technology allows traders to improve their stock management and theft prevention. On the other hand, these smart chips, if not deactivated upon purchase, may track consumers' behaviour [lo que no es posible en programas completos de alimentación saludable, pues es necesario saber qué alimento ha adquirido el consumidor para tener en cuenta sus propiedades]. The double-edged sword character of RFID tags is a known concern. In past years, the EU legislators commissioned data protection impact assessments to ensure sufficient consumer protection when traders use the RFID".

personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización".[9]

En el año 2018, el lector ya tiene en mente a qué concepto nos estamos refiriendo: *Big Data*. Pero la frase es de 1983, del Tribunal Constitucional Federal Alemán en su famosa Sentencia BvR 209/83 de 15 de diciembre, en la que se pueden encontrar de forma preclara las auténticas vigas maestras que sostienen el "derecho a la autodeterminación informativa" –*Recht auf informationelle Selbstbestimmung*– y sus implicaciones no solo para el derecho a la intimidad, sino, aún más allá, para la verdadera existencia de libertad, con implicaciones que no solo alcanzan a la autodeterminación informativa en sí misma (entendida como protección de datos de carácter personal en sentido estricto), sino también a la libertad individual y al libre desarrollo de la personalidad, núcleos irrenunciables del moderno Estado Social. En palabras del Tribunal (fundamento jurídico segundo): "En la clave de bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre".

Observemos estas ideas a la luz del progreso tecnológico, refiriéndonos, de modo sucinto, únicamente a potencia de procesamiento y capacidad de almacenamiento. Para ilustrar la evolución, tan solo a nivel de usuario, en enero de 1984 se lanzó el ordenador Macintosh 128k, con una CPU Motorola 68000, de 7'8336 Mhz, y una memoria de 0'125 Mb (128 kib, de ahí su nombre). Hoy día, un teléfono móvil de gama media presenta procesadores multinúcleo y multihilo de más de 2000 Mhz[10] y memorias de más de 2048 Mb (durante este año y el que viene se popularizarán los 8192 Mb para teléfonos 5G[11]), solo de memoria RAM, con almacenamientos que superan con facilidad los 128.000 Mb. De acuerdo con los datos facilitados por Cisco,

---

[9] Extracto de la traducción y análisis de Daranas, Manuel: "Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana", *Boletín de Jurisprudencia Constitucional*, Dirección de Estudios y Documentación del Congreso de los Diputados, Tomo IV (Jurisprudencia Constitucional Extranjera), Núm. 33, Madrid, 1984, pp. 126-170. El extracto citado corresponde a la página 153.

[10] Los megahercios no son, *per se*, una medida de potencia, sino de frecuencia de reloj. La potencia bruta depende de muchos otros factores, como la arquitectura del hardware, el tipo de instrucciones que se ejecutan en el mismo, etc. Un ejemplo de esto son las tarjetas gráficas y el hardware ASIC para minado.

[11] http://www.europapress.es/portaltic/gadgets/noticia-samsung-desarrolla-primera-memoria-lpddr5-dram-moviles-alcanza-gigabits-soporta-5g-20180717165509.html [Última consulta: 5 de agosto de 2018]. Lo cierto es que su fabricación e implementación para dispositivos móviles comenzó hace ya 4 años, en 2014: https://www.androidsis.com/samsung-ram-8gb/ [Última consulta: 5 de agosto de 2018].

en 2016 se transmitieron más de 1'2 zettabytes (10^{21} bytes, el penúltimo orden de magnitud de datos creado, recogido en el Sistema Internacional de Medidas, siendo el último el yottabyte) por internet, y se espera que en 2021 se alcancen los 3'3 Zbytes[12].

De todo lo anterior se colige –y esto es lo que se trataba de ilustrar–, que si ya en 1983 el Tribunal Constitucional alemán pudo observar la problemática de la creación de perfiles gracias al "*aumento de la capacidad computacional*", imaginemos cuál es su potencial 35 años después, máxime a la luz de las proporciones de almacenamiento y procesamiento[13] –*Big Data*– apenas expuestas *grosso modo*.

Ir contra el progreso tecnológico es de todo punto fútil y absurdo, como la historia ya nos ha enseñado. En esta nueva era, el anhelo de un hermetismo absoluto de nuestros datos no es realista, ni conduce a ningún sitio, toda vez que el *Big Data* y el tratamiento de datos ya se encuentran plenamente instaurados entre nosotros[14]. Es el presente y el futuro. La sociedad de la información y el medio digital forman una unidad con la idiosincrasia y el *modus vivendi* del siglo XXI.

---

12 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html [Última consulta: 5 de agosto de 2018]. Para mantener la proporción en las cifras, 1'2 zettabytes equivalen a 1.200.000.000.000.000 megabytes (1'2 trillones de megabytes).

13 Hilbert, Martin / López, Priscila, "The World's Technological Capacity to Store, Communicate, and Compute Information", *Science*, Vol. CCCXXXII, Núm. 6025 (abril), 2011, pp. 60-65. Disponible en: http://science.sciencemag.org/content/332/6025/60 [Última consulta: 5 de agosto de 2018]. Siguiendo esta información, en términos globales, se calculaba que la capacidad de almacenamiento mundial pudo alcanzar en el año 2007 los 290.000.000.000.000 Mbytes ($2'9 \times 10^{20}$ bytes) óptimamente comprimidos, comunicar casi 2.000.000.000.000.000 de Mbytes (2×10^{21} bytes) y realizar 6.400.000.000.000.000.000 (6.4×10^{18}) instrucciones por segundo en computadoras de propósito general a nivel usuario (es decir, sin contar equipos especializados, superordenadores, etc.). La capacidad informática de propósito general creció a una tasa anual del 58% entre 1986 y 2007. Diez años más tarde, se han popularizado *smartphones*, los sistemas de almacenamiento diminutos como las microSD con una capacidad máxima a nivel usuario de 520.000 Mbytes por unidad, procesadores multinúcleo de 64 bits, comunicaciones de banda ancha alámbrica e inalámbrica (VDSL, FTTH, 5G), etc.

14 Davara Fernández de Marcos, Isabel, *Hacia la estandarización de protección de datos personales,* Ed. La Ley, Las Rozas, 2011, p. 8. Dada la amplitud del concepto tratamiento, como bien señala la autora: "La realidad es que actualmente no existe actividad, pública o privada, comercial o no, que pueda sobrevivir sin tratamiento de datos de carácter personal (administrados, clientes, personal, etc.)".

Por ello, mi posición es que el debate no debe sustentarse sobre visiones catastrofistas[15] en cuanto a las posibilidades de la tecnología digital –cuyos aspectos positivos están resultando revolucionarios para la humanidad–, ni tampoco caer en la ingenuidad de que una normativa garantista como el RGPD[16] nos protege de todo riesgo aparejado al tratamiento de datos. En su lugar, apuesto por potenciar un auténtico control de los mismos, que exige dotar de una mejor educación y concienciación sobre su uso y sus aplicaciones; a la par que se aborda una indemorable mejora de la obtención del consentimiento, que se concreta en el fin de las largas condiciones generales[17] de privacidad en pos de una información más clara[18], que permita diferenciar distintos tipos de datos y sus respectivos tratamientos[19], dando

---

[15] Fernández Agis, Domingo, "Humanismo, posthumanismo e identidad humana", *Ius et Sciencia: Revista Electrónica de Derecho y Ciencia*, Vol. IV, Núm. 1, 2018, p. 7: "*Se trata del incremento logarítmico del poder de la tecnología. La interpretación que se da a estos aconteceres es de muy diverso signo, abarcando desde el optimismo ingenuo al catastrofismo más exagerado. En medio de tanta confusión y conflicto de interpretaciones, hemos de considerar que ésta sí que es una característica esencial de nuestro presente y que afecta directamente a lo que somos, a cómo nos definimos y afrontamos la vida. Así pues, nuestra vida, en todos sus aspectos está mediada por la tecnología*". Disponible en: http://institucional.us.es/iusetscientia/index.php/ies/article/view/139 [Última consulta: 6 de agosto de 2018]

[16] 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), Diario Oficial de la Unión Europea, L 119, de 4 de mayo de 2016. Páginas 1-88.

[17] Parliament House of Commons. Science and Technology Committee, *Responsible Use of Data. Fourth Report of Session 2014-15*, The Stationery Office Limited, Londres, Reino Unido, p. 21. Parte del problema subyace en lo que, con gran claridad, explicó Carl Miller ante la House of Commons británica: "*ha habido pocos incentivos para que muchos proveedores de plataformas hagan cualquier cosa que no sea emitir documentos de 100 páginas, porque todos hacen clic en 'Sí' y, para cambiar el status quo, la presión 'debería aplicarse desde fuera de la empresa'*". El mismo, añadió una estadística de acuerdo con la cual: "si lees todos los términos y condiciones [que aceptas] en Internet pasarías un mes cada año en ello". Carl Miller compareció ante el Parlamento Británico en calidad de Director de Investigación en el Centro para el Análisis de Redes Sociales Demos. La referida problemática ha sido denunciada también desde otros sectores, como la asociación de consumidores australianos CHOICE, a quienes tomó casi 9 horas leer los términos y condiciones de Amazon (léase con la debida cautela): https://www.choice.com.au/consumerlaw [Última consulta: 2 de agosto de 2018]. El proceso fue supuestamente documentado en vídeo y resumido en: https://www.youtube.com/watch?v=sxygkyskucA [Última consulta: 2 de agosto de 2018].

[18] Considerando 39: "(…) El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro".

[19] Considerando 32: "(…) El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos".

lugar a permisos más estratificados. Con ello, se permitiría al individuo llevar a cabo un verdadero control de sus datos, cumpliendo con lo prescrito por el considerando 32 RGPD. Lo que se persigue es empoderar a las personas[20] no solo como usuarios o consumidores, sino, por su potencial alcance, también como ciudadanos. Se trata de concebir y promover el control de los propios datos como un verdadero ejercicio, inteligente y consciente, de auténticos derechos fundamentales del individuo.

En definitiva, el objetivo es articular la capacidad de poder llevar a la práctica un derecho fundamental de un modo tan celoso y fuerte como cada individuo considere respecto de su propia esfera de privacidad. Este es el *leitmotiv* que debe presidir, a mi juicio, la supervisión de las operaciones en las que se utilizan datos de carácter personal –tratamiento–, principalmente, su obtención con un consentimiento adecuado, su cesión, su combinación, y la creación de perfiles. Al fin y al cabo, cuando defendemos el tratamiento de nuestros datos, en especial biosanitarios, estamos salvaguardando el núcleo más íntimo[21] de nuestra personalidad, de nosotros como individuos. La renuncia a ello desplaza ese beneficio, de la esfera del individuo, hacia la esfera de las compañías o agentes del mercado que los tratan en todo tipo de negocios como una nueva fuente que permite maximizar sus beneficios[22], pues esa es su propia razón de ser.

Cualquier otra excusa enmascara esta realidad. Las compañías privadas operan en el mercado para obtener ganancias, no para generar mercedes a la ciudadanía, por lo que su objetivo es claramente privado y, por tanto, resulta

---

[20] Fernández López, Juan Manuel, "Principio de consentimiento: Título II. Principios de la Protección de Datos. Artículo 6", *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, Troncoso Reigada, Antonio (Coord.), Thompson Civitas, 2010, p. 453.

[21] Rebollo Delgado, Lucrecio, *Vida privada y protección de datos en la Unión Europea*, Ed. Dykinson, Madrid, 2008, pp. 99-100: "La concepción de derecho a la intimidad que une la definición objetiva y subjetiva nos parece hoy la más acorde tanto con la idea de derecho a la intimidad, como con las necesidades de nuestro ordenamiento jurídico. Se debe ello en esencia a la evolución del derecho a la intimidad, el cual ha ido ensanchando sus límites y su configuración partiendo del núcleo de ser un derecho de defensa y de exclusión o no intromisión, hasta convertirse en un derecho que posibilita el control de aquello que al individuo afecta y debe ser controlado y modulado por él".

[22] En enero de 2017, la agencia de noticias Europa Press se hacía eco de un informe de la consultora KPMG, en el que el 83% de los directivos de la industria de la automoción afirmaba que los fabricantes de vehículos obtendrán ingresos de la explotación de los datos. http://www.europapress.es/motor/coches-00640/noticia-diesel-primera-tecnologia-desaparecer-dicen-directivos-automocion-20170103105321.html [Última consulta: 26 de julio de 2018].

difícil de calificar como "interés general"[23], expresión con la que el RGPD se refiere reiteradamente a los posibles tratamientos de datos relativos a la salud. También la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales 3/2018[24] profundiza, en su Disposición adicional decimoséptima, en el tratamiento de datos de salud para investigación e interés general, introduciendo el control de comités de ética en la investigación pública, y donde exige la incorporación "entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679" –apartado 2, letras g) y h)–.

Sin perjuicio de lo anterior, todo ello no es ningún impedimento al mercado y a la economía de los datos. ¿Puede el individuo transar sobre sus datos a cambio de bienes o servicios? Evidentemente, y son *res intra-commercium*[25], pero no solo debe ponderarse su valor económico e industrial, sino también el impacto social que tal mercadeo trae consigo. Convertir millones de perfiles de individuos en datos, y a efectos prácticos en muchas ocasiones, equivalentes a una mercancía, constituye un ejercicio de deshumanización[26], especialmente en materia sanitaria, aspecto que no podemos perder de vista. En cualquier caso, el individuo debe ser libre en su decisión y plenamente consciente de la misma, y para ello se necesita más pedagogía, así como una mejor información al momento de otorgar su consentimiento, que le dote de verdadero poder de decisión. Como recoge el considerando 4º del RGPD: "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad"[27], lo que constituye un apunte de marcado carácter teleológico para la interpretación de la norma.

---

[23] Los ciudadanos pueden querer ceder sus datos para investigación pública, a cambio de poder beneficiarse de nuevos tratamientos el día de mañana o, al igual que ocurre con las donaciones de sangre, médula, órganos, etc. por puro altruismo. Pero no estarán dispuestos a hacer tales cesiones para favorecer el lucro de terceros y a su propia costa.

[24] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
Publicado en el BOE núm. 294, de 6 de diciembre de 2018.

[25] De Franceschi, Alberto, *European contract law and the digital single market*, Intersentia, Cambridge, Reino Unido, 2016, p. 5.

[26] De Lecuona Ramírez, Itziar / Villalobos-Quesada, María, "El valor y el precio de los datos personales de salud en la sociedad digital", *El cuerpo diseminado: estatuto, uso y disposición de los biomateriales humanos,* García Manrique, Ricardo (Coord.), Aranzadi, Cizur Menor, España, 2018, pp. 171-190.

[27] A lo que añade: "(…) en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de

2. Los datos biosanitarios en línea: sensibilidad, especial consideración y alto valor

El RGPD, cuando se refiere a los datos de salud a lo largo de todo el texto, tanto en los considerandos como en el articulado, con frecuencia lo hace vinculado a otros conceptos como "interés general", "salud pública" o "investigación", y, en gran medida, conectado a una concepción médico-asistencial del dato biosanitario. Sin embargo, a pesar de que la mayor parte de la información biométrica que se recaba a través de aplicaciones y *wearables*, entra dentro de la definición de dato relativo a la salud o dato biométrico, la finalidad para la que los tratan, nada tiene que ver, *a priori*, con las referidas nociones.

El RGPD en su art. 2, dedicado a definiciones, distingue entre "datos biométricos" y "datos relativos a la salud"[28], que serán las dos categorías en las que podrán clasificarse los datos que se obtienen a través de *wearables*, pulseras, teléfonos móviles, etc. Los primeros, son aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Estos datos son recogidos, por ejemplo, por nuestros teléfonos móviles, como medida de seguridad para desbloquearlos; o por nuestras *tablets*, para identificar a un usuario[29] y darle acceso al sistema cargando su configuración.

Por su parte, los datos relativos a la salud se definen como: "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud". Pulsaciones, porcentaje de grasa corporal, o ritmos de sueño son algunos de los ejemplos que encajan aquí y que reseñaremos en este trabajo.

---

pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística".

[28] Barral Viñals, Inmaculada, "Datos relativos a la salud e historia clínica: La confidencialidad de los datos médicos", *Protección de datos personales en la sociedad de la información y la vigilancia,* Llácer Matacás, María Rosa (Coord.), Ed. La Ley, Las Rozas, Madrid, España, 2011. En sus páginas 352 y 353 puntualiza las diferencias entre el genérico "dato médico" y el más específico, "dato relativo a la salud", más correcto y preciso.

[29] https://developer.apple.com/design/human-interface-guidelines/ios/user-interaction/authentication/ [Última consulta: 19 de agosto de 2018].

Más allá de esta debida reseña al tenor literal de ambos conceptos, lo más importante es que ambos ostentan la categoría de "datos especialmente protegidos" en el art. 9.1. Por consiguiente, su tratamiento, como regla general, se encuentra prohibido. Solo podrá salvarse si "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados". Las exigencias en la obtención del consentimiento son altas en general en el RGPD, más aún si cabe cuando nos encontramos ante una categoría de datos sensibles, cuyo tratamiento se encuentra prohibido como regla general. Es ahí donde encontramos que se produce la quiebra de las exigencias del RGPD, que abordaremos con posterioridad.

Una vez sentada su especial calificación desde un punto de vista puramente normativo, cabría preguntarse. ¿Cuál es su valor real? ¿De dónde se obtiene su utilidad económica? Algunos de los primeros ejemplos de venta de una base de datos de clientes en el medio online datan de principios de siglo, como los casos de living.com (2000), egghead.com (2001) y el más conocido, Toysmart[30]. En el año 2000, tras la quiebra de la empresa Toysmart, esta puso a la venta su base de datos, con 195.000 perfiles de clientes, incluidos menores. En un primer término, Disney, que ya era accionista de la compañía quebrada, se ofreció a pagar por ella 50.000 euros para su destrucción, si bien finalmente fue vendida a un tercero "de confianza" con el visto bueno de la fiscalía y del juzgado donde se estaba liquidando la empresa[31]. Más recientemente, tras la bancarrota de la empresa Radioshack (en 2015), la compañía General Wireless compró algunos de los bienes intangibles de la empresa por 26'2 millones de dólares[32], incluyendo 67 millones de nombres

[30] Kelly, Eileen P. / Erickson, G. Scott, "Legal and privacy issues surrounding customer databases and e-merchant bankruptcies: reflections on Toysmart.com", *Industrial Management & Data Systems*; Vol. CIV, Núm. 3/4, 2004, p. 209-217. P. 215: "The issue of personal, informational privacy is of growing concern as our society becomes more and more digitized. The value of personal information is dramatically highlighted in the commercial arena where information is a valuable and lucrative commodity. Online businesses have a particular need for, and ability to, acquire identifiable, individualized customer information. This treasure trove of information is a valuable asset that creditors can lay claim to in a bankruptcy proceeding".

[31] Carrol, Brian, "Price of privacy: selling consumer databases in bankruptcy", *Journal of Interactive Marketing*, Vol. XVI, Núm. 3 (verano), 2002, pp. 47-58. Argumenta este autor que el factor clave para evitar su venta indiscriminada fue que ambas páginas habían establecido cláusulas de privacidad en las que se comprometían a no vender la información de los clientes, y se pregunta qué hubiera pasado si hubieran sido redactadas de otro modo. Página 56: "Had living.com and Toysmart.com published very permissive privacy policies, the FTC and attorneys general likely would not have taken action".

[32] https://www.bloomberg.com/news/articles/2015-05-13/standard-general-bid-of-26-5-million-wins-radioshack-brand [Última consulta: 10 de septiembre de 2018]. Según

de consumidores[33] con 11 millones de direcciones postales[34], y en 2016 Sports Authority vendió su base de datos de clientes por 15 millones de dólares[35]. La solución más aceptada por los Juzgados viene siendo que las bases de datos no se entreguen íntegras al comprador, sino eliminando parte de ellas, a fin de no exponer por completo a los clientes ante el nuevo comprador.

En la actualidad, los datos biométricos y, en general, los relativos a la salud, son los más valorados en el mercado de datos. Como señala Elvy: "Antes de los avances tecnológicos del IoT, el acceso a los datos relacionados con la salud del consumidor generalmente se limitaba a los proveedores de servicios de salud y seguros. De manera similar, los datos biométricos, como los escaneos de huellas dactilares, podían acceder regularmente con regularidad solo las entidades gubernamentales o quizás algunos empleadores y la industria bancaria y de pagos. Hoy en día, las empresas, como Apple, usan datos biométricos en relación con sus productos. En la configuración del IoT, los datos biométricos y relacionados con la salud ya no se mantienen principalmente en un grupo selecto de entidades y proveedores tradicionales. En cambio, este tipo de datos ahora están más dispersos y disponibles para diversas entidades, incluidos minoristas, fabricantes y compañías de software y en línea, debido al uso que hacen los consumidores de dispositivos de IoT, aplicaciones de entrenamiento físico y otras aplicaciones móviles"[36]. A eso, añade otro factor importante: la información bancaria puede cambiarse (por ejemplo, si obtienen nuestro número de tarjeta de crédito, podemos

---

reporta The Wall Street Journal en su edición de 28 de abril de 2015, durante la tramitación de la liquidación judicial de la empresa, se detalló que la base de datos contenía más de 200 tipos diferentes de datos, incluyendo hábitos del consumidor, lugar donde hizo las compras, si pagó en metálico o con tarjeta de crédito, si usó cupones de descuento y qué cupones fueron, etc. Documento obtenido a través de la base de datos proquest: https://search.proquest.com/docview/1676155404?accountid=14501 [Última consulta: 10 de septiembre de 2018].

33 https://www.reuters.com/article/us-radioshack-bankruptcy/u-s-judge-rules-radioshack-ip-auction-was-fair-idUSKBN0O52I120150520 [Última consulta: 10 de septiembre de 2018].

34 https://www.theguardian.com/business/2015/may/18/bankrupt-radioshack-selling-customer-data-names-addresses [Última consulta: 10 de septiembre de 2018].

35 Elvy, Stacy-Ann, "Commodifying consumer data in the era of the internet of things", *Boston College Law Review*; Vol. LIX, Núm. 2, 2018, pp. 423-522. P. 431: "In another example, in 2015 RadioShack filed for bankruptcy and among the company's assets were "117 million customer records" that included personally identifiable information, such as dates of birth, credit and debit card numbers, names, and physical and email addresses. Standard General eventually acquired the company and its customer database. Similarly, in 2016 Sports Authority filed for bankruptcy and sold its customer database for a winning bid of $15 million".

36 Ídem, p. 428. Traducción propia.

cancelarla y pedir otra nueva), pero los datos biométricos no (por ejemplo, la huella dactilar).

En 2015, la compañía norteamericana McAfee, especializada en ciberseguridad, publicó su informe "*Hidden Data Economy Report Exposes Price Points for Stolen Data*"[37], en el que afirmó que el valor de estos oscilaba entre 10 y 20 veces más en el mercado negro que los números de tarjeta de crédito. Más revelador aún, es que explica que no nos encontramos ante una realidad extraordinariamente clandestina, sino todo lo contrario: "El título de este informe sugiere que existe una puerta escondida en un mercado subterráneo para productos terribles que no son accesibles para nosotros muggles*. En realidad, este mercado no está tan bien escondido como nos imaginamos, y ciertamente no requiere previo conocimiento de un 'piso franco'**. [En nuestro informe] Cibercrimen Expuesto: Cibercrimen-como-servicio se destaca cuán accesibles son estos productos, herramientas y servicios para cualquier persona con un navegador"[38]. A mayor abundamiento, añaden: "Este mercado negro ha evolucionado hasta incorporar para su venta o alquiler casi todos los productos que puedan obtenerse como resultado de la ciberdelincuencia. (…) El crecimiento de una economía de tipo "as-a-service" en todos los componentes de un ataque (investigación, herramientas de cibercrimen e infraestructura) como servicios sigue expandiéndose, y ninguno más que hacking-as-a-service, en particular sobre cómo se lleva a cabo la puesta a disposición de los datos robados", para terminar afirmando que la "(…) apatía de las víctimas de una violación de datos, y en definitiva los datos de los sujetos cuya información se vende, pueden ser costosos".[39]

---

[37] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf [Última consulta: 5 de agosto de 2018].

[38] *Ídem*, p. 4, original en inglés: "*The title of this report suggests that there exists a hidden doorway into an underground marketplace for nefarious products that is not accessible to us muggles. In reality, this marketplace is not nearly as well hidden as we imagine, and it certainly does not require prior knowledge of a secret public house and its hidden courtyard*** [traducción adaptada]. Cybercrime Exposed: Cybercrime-as-aService highlights just how accessible these products, tools, and services are to anybody with a browser".

* El término "muggle" es importado de la cultura popular (en concreto, de la saga Harry Potter) y hace referencia a los humanos normales, sin habilidades excepcionales, y no conlleva ninguna connotación peyorativa, sino que se trata de un término meramente descriptivo. Se utiliza en este caso para designar a las personas que desconocen el funcionamiento detallado de internet.

[39] *Ibídem,* traducción propia.

El Departamento de salud y servicios sociales de Estados Unidos[40] tiene habilitado un portal en línea donde se publican todos los incidentes de ciberseguridad relativos a registros sanitarios que hayan afectado a más de 500 personas, lo que incluye pérdidas de dispositivos o errores de red, pero también actos de *cracking* (más correcto que *hacking*[41]) o robos de información. Una visita a su página web[42] muestra una preocupante cantidad de ataques, lo que pone de manifiesto, una vez más, el valor y el interés que despierta la obtención de los datos sanitarios. Prueba evidente de ello, podemos encontrarla en el mercado de la Deep Web conocido como "TheRealDeal Market" –hoy día caído o trasladado[43]–. En junio de 2016, el hacker anónimo "thedarkoverlord" puso a la venta más de 9 millones de registros sanitarios (trufados de datos personales como nombre, apellidos, dirección, e-mail, número de teléfono, etc.) obtenidos de las bases de datos de una compañía aseguradora estadounidense, a la venta por cerca de medio millón de dólares (750 bitcoins de la época)[44].

Más recientemente, en septiembre de 2017, la Sociedad Española de Informática de la Salud (SEIS) celebró en Mérida la VII reunión del Foro para la Gobernanza de las TIC en Salud, donde se cuantificó el valor de los datos de salud en 20 dólares, mientras que los de tarjetas de crédito se valuaron en torno a los 10 a 15 dólares[45], según la información facilitada por Javier Jarauta en dicho encuentro. Otra cifra interesante extraída del mismo foro, que indica la relevancia y el valor que pueden proporcionar los datos sanitarios, es que el 26% de los ciberataques se producen contra servicios de salud.

---

40 U.S. Department of Health and Human Services.

41 Como explica la firma de ciberseguridad Avast: "Mientras que el hacking consiste en burlar los sistemas de seguridad para obtener acceso a los equipos informáticos (lo que puede ser bueno o malo), el cracking consiste en lo mismo, pero con intenciones delictivas. La opinión general es que los hackers construyen, mientras que los crackers destruyen. En concreto, los crackers se suelen dedicar a robar números de tarjetas de crédito, diseminar virus, destruir archivos o recopilar datos personales para venderlos posteriormente". https://www.avast.com/es-es/c-cracking [Última consulta: 5 de agosto de 2018].

42 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [Última consulta: 5 de agosto de 2018].

43 http://trdealmgn4uvm42g.onion [Última consulta: 5 de agosto de 2018]. Advertencia: para abrir este enlace se requiere el uso del navegador Tor para dark web, y su uso está totalmente desaconsejado para personas no expertas. No obstante, esta URL es antigua y podría encontrarse caída o trasladada a otro dominio.

44 https://www.deepdotweb.com/2016/06/28/now-9300000-healthcare-insurance-database-sold/ [Última consulta: 5 de agosto de 2018].

45 https://www.diariomedico.com/profesion/el-mercado-negro-de-los-datos-de-salud.html [Última consulta: 5 de agosto de 2018].

También en 2017, la compañía de ciberseguridad japonesa Trend Micro elaboró un informe denominado "The Expansion of Cyber Underground Goods to Electronic Health Data"[46]. La compañía cifra en más de 113 millones la cantidad de datos sanitarios sustraídos solo en el año 2015. El informe se centra, en primer término, en "(…) entender cómo los registros médicos robados se monetizan después de su sustracción, qué tipos de datos se roban, por cuánto se venden en los mercados negros, y cómo los cibercriminales hacen uso de ellos"[47]. De su atenta lectura, se desprende que su valor económico radica en su potencial defraudador, y no en la información puramente biosanitaria, con la salvedad de la obtención de recetas de medicamentos restringidos. En su segunda parte, se pone de relieve cómo la conexión de todo tipo de aparatos susceptibles de recibir y enviar datos e instrucciones en red sin necesaria intervención humana, fenómeno denominado conocido como Internet of Things (IoT), y que se potenciará exponencialmente[48] con la llegada de la tecnología 5G[49], conlleva el registro de una inmensa cantidad de datos, a la vez que puede exponerlos de forma insegura en la red. En la página 18 del informe, se hace referencia al buscador especializado Shodan, y cómo este puede brindar con facilidad información recogida por los referidos dispositivos, tal como los servicios o aplicaciones ejecutándose en los mismos, la estructura del sistema de archivos, carpetas (cuya mera denominación es susceptible de reflejar datos personales, por ejemplo, si se abre una carpeta con el número de la seguridad social, DNI, etc.), dirección geográficas y dirección IP, etc.

Si esta realidad del mercado negro de los datos es ya innegable, menos aún lo es el interés que este tipo de datos representa para bancos, aseguradoras, farmacéuticas, y muchos otros operadores que actúan de forma directa o indirecta sobre el mercado de la salud. En palabras de Beltrán Aguirre: "En el ámbito privado, la industria farmacéutica, la industria alimentaria, las compañías aseguradoras y los bancos con sus sistemas de evaluación automática de solicitudes de seguros, operaciones de créditos, préstamos, etc., están muy interesados en estas bases de datos para crear perfiles de

---

46 https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf [Última consulta: 6 de agosto de 2018].

47 *Ídem*, p. 3.

48 Rita Palattella, Maria *et ál.*, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models", *IEEE Journal on Selected Areas in Communications*, Vol. XXXIV, Núm. 3 (marzo), 2016, pp. 510-527.

49 Lemstra, Wolter, "Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implication", *Telecommunications Policy,* Vol. XLII, 2018, pp. 587–611. En particular, p. 608.

riesgo, y están dispuestos a pagar muy bien por acceder a ellas"[50]. En esta misma línea, De Lecuona Ramírez y Villalobos-Quesada: "Es habitual que esta información sea liberada, con o sin conocimiento del titular de los datos, a terceros que acumulan y ponen precio a esos datos, generando nuevos modelos de negocio"[51].

Ello da cuenta de la doble dimensión de valor que presentan los datos sanitarios, así como de su auténtica relevancia económica: en primer lugar, por su propio valor intrínseco en el mercado, y en segundo, por su capacidad de brindar información y patrones de negocio explotables gracias al Big Data. Veamos un ejemplo claro en un caso real. El 11 de abril de 2018, el diario Expansión recogía en su edición digital el lanzamiento de un nuevo seguro de El Corte Inglés con el siguiente titular: "El Corte Inglés lanza un seguro de vida que 'paga' a sus titulares por andar"[52]. En el artículo, se recogen algunas de las claves de cómo se relaciona la actividad del individuo con su compañía aseguradora. Se denomina VidaMovida, y está dirigido a personas "entre 18 y 65 años", no fumadores o que lleven más de dos años sin fumar, ya que "persigue premiar a aquellos que se preocupan por su bienestar". Siguiendo esta información, entre 18 y 35 años, andar 10.000 pasos al día (el máximo), generará para el usuario un bono de compras en tiendas El Corte Inglés por un valor equivalente al 41% de su prima. Entre 35 y 39 años, la bonificación máxima será del 33 % de la prima, y para los que tienen entre 40 y 44 años del 24%. No se menciona nada sobre la franja de edad hasta los 65 años. De acuerdo con las declaraciones del director comercial de El Corte Inglés Seguros, Juan Manuel de Prada a dicho diario: "confían que será el producto estrella del año que les permitirá alcanzar el objetivo de superar las 100.000 contrataciones de seguros de vida y accidentes en 2018".

El blog de Seguros El Corte Inglés ofrece más información sobre este producto[53]. Según se recoge su propia página web: "¿qué es exactamente lo que podemos conseguir si alcanzamos la media de 10.000 pasos al día que proponen? Nada más y nada menos que una recompensa de cuarenta euros anuales que podrás canjear por una Tarjeta Regalo El Corte Inglés para comprar lo que quieras". Las recompensas económicas son: "4 euros

[50] Beltrán Aguirre, Juan Luis, "Tratamiento de datos personales de salud: incidencia del Reglamento General de Protección de Datos", *Salud electrónica. Perspectiva y realidad,* Pérez Gálvez, Juan Francisco (Dir.), Tirant lo Blanch, Valencia, 2017, p. 121.

[51] De Lecuona Ramírez, Itzíar / Villalobos-Quesada, María, *op. cit.* Versión Proview.

[52] http://www.expansion.com/empresas/banca/2018/04/10/5accd666ca4741fa528b4635.html [Última consulta: 10 de septiembre de 2018].

[53] https://seguros.elcorteingles.es/blog/vida-saludable/vidamovida-el-seguro-de-vida-que-te-paga-por-andar [Última consulta: 10 de septiembre de 2018].

al trimestre por una media de 4.000 pasos hasta los 10 euros por una media de 10.000 pasos, que equivale a 7 kilómetros".

Si tenemos en cuenta que 10.000 pasos equivalen a unos 7 kilómetros diarios, esto equivaldría a 210 kilómetros caminados al mes. Dado que el máximo son 40 euros anuales, el beneficio por dichos 210 kilómetros mensuales (más de 2.500 km al año) son 3'33 euros para los usuarios. Para dar cuenta de los pasos dados, los contratantes deberán "sincronizar [s]us pasos con las apps de Google Fit, Apple Health o de cualquiera aparato de medición de actividad disponible en el mercado". Gracias a este producto, El Corte Inglés Seguros espera "que si el asegurado mantiene unos hábitos de vida saludables a largo plazo se reducirá la siniestralidad del seguro, aunque no ha cuantificado cuál podría ser la reducción en el caso de VidaMovida", tal y como se recoge en la citada noticia del diario Expansión.

Aseguradoras, farmacéuticas, sector bancario[54] y todo tipo de empresas (como acabamos de observar en el caso de El Corte Inglés) los explotan como parte de su negocio con creciente importancia[55]. Siguiendo a efectos ilustrativos el ejemplo del seguro expuesto, la empresa (Inithealth SL) que provee la plataforma sobre la que opera la App explica en su página web cuál es el objetivo de estas prácticas: "Inithealth Affinity Fideliza a tus clientes a través de la salud y el bienestar. Inithealth Affinity es la plataforma más completa para la gestión de la salud y el bienestar, 100% personalizable y adaptable a las necesidades de la compañía; care plans personalizados, conexión de dispositivos médicos, wearables y sistemas de gamificación y engagement"[56]. Se encuentra dirigida a "Grandes Colectivos, Entidades Aseguradoras, Entidades financieras y Sector Sanitario". En otras palabras: esta finalidad puramente comercial no encaja con las nociones de interés general o asistencial que presiden las concepciones relativas a la protección de datos sobre la salud en el RGPD.

---

54 https://www.bbva.com/es/empresas-deben-entender-big-data-moda/. "Contar con la capacidad de extraer la mayor cantidad de datos de los clientes y usarlos para entender los comportamientos y gustos del consumidor y cómo hacer uso de manera acertada (…)". [Última consulta: 3 de septiembre de 2018].

55 Guama Morales, Sonia Carolina, "Estudio comparativo de métodos existentes para integrar la información estructurada y no estructurada de una industria enfocado en la generación de conocimiento, desde la perspectiva de una solución integral de Big Data", repositorio digital de postgrados (Maestría en Gerencia de Sistemas y Tecnologías de la Información) de la Universidad de las Américas, Chile, 2015. Disponible en línea en: http://dspace.udla.edu.ec/handle/33000/3385 [Última consulta: 3 de septiembre de 2018].

56 https://www.inithealth.com/ [Última consulta: 11 de septiembre de 2018].

Evidentemente, el título que habilitará para llevar a cabo este tipo de tratamientos será el consentimiento. El problema que aquí se presenta (y es muy habitual en el ámbito digital) es si se recabó en bloque, es decir, la aceptación de todas las cláusulas mediante una única casilla y botón de aceptación. A mi juicio, los consentimientos recabados con tal técnica podrían adolecer de un posible vicio, debido a que el art. 9.2 a) RGPD establece que, en materia biosanitaria, deberá ser "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados". Siendo datos sensibles, no podemos interpretar este artículo desoyendo la exigencia del considerando 32 cuando prescribe: "Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos". Y no de cualquier manera, sino bajo unos férreos estándares de claridad y transparencia previstos, por ejemplo en el considerando 39: "El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro"; el considerando 58: "El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice", a lo que vale la pena añadir: "Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber"; y, finalmente, el considerando 60: "Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines", exigencias que, tras una atenta lectura más allá de estos breves extractos, verifican la existencia de un estándar muy alto no solo en el trámite de información ofrecida para recabar el consentimiento del afectado, sino en el cumplimiento de los arts. 5.1 –principios del tratamiento: –, 6.1 –licitud del tratamiento– y 7.2 –condiciones para el consentimiento– del RGPD .

Recordemos, además, que la finalidad del tratamiento de estos datos biosanitarios no es médico-asistencial. Se opera sobre ellos con fines comerciales, como, por ejemplo, para medir riegos y aplicar patrones. Es más, cabe preguntarse: cuando se incluye la cláusula de conservación al objeto de responder a posibles requerimientos ¿puede invocarla el propio responsable para defenderse de una demanda presentada por el interesado? Por ejemplo, en base a ella, podrían conservarse los datos y aportarlos a la causa para alegar un incumplimiento contractual o un comportamiento negligente del usuario. En el caso del seguro, podría saberse si no salió a dar paseos o si llevó a cabo un comportamiento sedentario que ha podido ser causa o agravante de una enfermedad. Una aplicación práctica es el estudio de riesgos asociados

al estilo de vida del asegurado de acuerdo con sus movimientos crediticios, como ya viene haciendo Carolinas Healthcare en Estados Unidos[57]. Y estos ejemplos son vitales: cuando salir o no dar un paseo empieza a tener relevancia contractual, o en tu rating crediticio[58], o en tus coberturas de seguro de vida o de salud, queda patente que la libertad del individuo ya no es tal.

De todo lo anterior se colige una pregunta muy evidente, conectada con el *leitmotiv* de este trabajo: ¿Están tratando adecuadamente nuestros datos sanitarios y biométricos todas aquellas empresas que los recaban? ¿Están poniendo medidas adecuadas de ciberseguridad? ¿Están implantando políticas efectivas de *privacy by design* como exige el art. 25 RGPD? ¿Están recabando adecuadamente el consentimiento necesario para un tratamiento que se encuentra prohibido por defecto? ¿Sirve en datos especialmente sensibles fuera del ámbito asistencial con un consentimiento genérico, a través de un botón, con el que se acepta todo un pliego de condiciones de privacidad?

Lo que aquí trata de significarse, y hemos tratado de dejar sentado, es que los datos sanitarios y biométricos gozan de un alto valor económico, tanto en el mercado negro como para los modelos de negocio de grandes empresas, lo que refleja no solo su importancia, sino también el celo que deben tener las personas físicas a la hora de dar su consentimiento para el tratamiento de este tipo de datos. El RGPD también confiere un alto grado de sensibilidad a estos datos, pero se ha ocupado principalmente de regular sus efectos en los campos de la investigación o la salud pública, desde un punto

---

57 https://www.bloomberg.com/news/articles/2014-07-03/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick [Última consulta: 1 de agosto de 2018]. "The company purchases the data from brokers who cull public records, store loyalty program transactions, and credit card purchases. (…) Information on consumer spending can provide a more complete picture than the glimpse doctors get during an office visit or through lab results, says Michael Dulin, chief clinical officer for analytics and outcomes research at Carolinas HealthCare. The Charlotte-based hospital chain is placing its data into predictive models that give risk scores to patients. (…) The system may also look at the probability of someone having a heart attack by considering factors such as the type of foods she buys and if she has a gym membership. 'The idea is to use Big Data and predictive models to think about population health and drill down to the individual levels,' he says".

58 Goozner, Merril, "Do you know your healthcare credit score?", Modern Healthcare, Vol. XLVI, Núm. 23 (junio), 2016, p. 40: "A report by the Consumer Financial Protection Bureau 18 months ago documented the toll taken by this type of debt. The agency found 20% of all consumer credit report scores--that's 43 million people--were lowered by unpaid medical debt. Virtually all of those bills were reported to credit bureaus by collection agencies, not directly by doctors and hospitals. It doesn't matter that the median unpaid bill was $207 for medical debt compared with $366 for nonmedical bills (the averages were $579 and $1,000, respectively). Credit bureaus do not distinguish between an unpaid hospital or physician deductible and an unpaid cellphone bill".

de vista esencialmente asistencial o médico, lo que no se ajusta a esta realidad económica de nuestros días que venimos exponiendo. Todo lo anterior crea un escenario en el que el consentimiento expreso que exige el RGPD, debe venir obtenido a través de una fase de información acorde a esta realidad, pues de lo contrario, sería incompleta y no transparente para el interesado, no superando el listón marcado por el Reglamento.

3. Los *wearables*, el granjeo constante de datos y monitorización de actividades. ejemplos reales a la luz de dispositivos en el mercado

IBM presentó en 2018 su nuevo ordenador de 1 milímetro cuadrado, que cabe con facilidad en la yema de un dedo, cuyo coste de producción es de 10 céntimos[59], y cuya finalidad es "*monitorizar, analizar, comunicar e incluso actuar sobre los datos*"[60]. Su potencial es extraordinario para multitud de tareas, incluidas aquellas que conllevan el tratamiento de datos relativos a la salud o biométricos.

Los *wearables* y las *APPs*[61] de mHealth[62] han llegado para quedarse, y de acuerdo con las cifras de la consultora International Data Corporation[63], para

[59] Diario El Mundo, edición de 20 de marzo de 2018: "IBM crea el ordenador más pequeño del mundo: abulta menos que un grano de arroz". http://www.elmundo.es/tecnologia/2018/03/20/5aafe6b846163f5c4c8b45d5.html [Última consulta: 26 de julio de 2018].

[60] https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/ [Última consulta: 26 de julio de 2018]: "The world's smallest computer is an IBM-designed edge device architecture and computing platform that is smaller than a grain of salt will cost less than ten cents to manufacture and can monitor, analyze, communicate, and even act on data. It packs several hundred thousand transistors into a footprint barely visible to the human eye and can help verify that a product has been handled properly throughout its long journey".

[61] Ramón Fernández, Francisca, "La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico", *Métodos de Información*, Vol. VIII, Núm. 14, 2017, p. 14. Esta autora se centra en los datos genéticos, y menciona aplicaciones como "*face2gene*", "*Smart phenotyping*", o "*better genetics*".

[62] Esto, junto con las APPs que les acompañan, y otra serie de APPs de salud que proliferan en las tiendas de aplicaciones de las compañías, han venido a ser denominadas como mHealth. Ochagavías Colás, Juan Ignacio, "Una panorámica de las nuevas tecnologías aplicadas al ámbito de la salud a propósito del m-Health y sus interacciones jurídicas", *DS: Derecho y salud*, Vol. XXVI, Núm. Extra 1 (Ejemplar dedicado a: XXV Congreso 2016: El avance de las Ciencias de la Salud y las incertidumbres del Derecho, 2016), p. 280. Disponible en línea en: http://www.ajs.es/revista-derecho-y-salud/una-panoramica-de-las-nuevas-tecnologias-aplicadas-al-ambito-de-la-salud-a-proposito-del-m-health-y-sus-interacciones-juridicas [Última consulta: 5 de septiembre de 2018].

[63] https://www.idc.com/getdoc.jsp?containerId=prUS42818517 [Última consulta: 3 de septiembre de 2018].

el año 2017 se esperaba la venta de 125'5 millones de wearables, con un incremento interanual del 20,4% tomando como referencia 104'3 millones de unidades vendidas en 2016. Según sus pronósticos, de ahí en adelante, el mercado de los wearables se duplicará hasta alcanzar un total de 240'1 millones de unidades en 2021, lo que representa una tasa de crecimiento anual acumulada del 18'2% durante este periodo quinquenal. Veamos algunos ejemplos reales de wearables y su capacidad para recabar y tratar datos.

Sirva como ilustración de todas las posibilidades que se abren la pulsera Simband, de la compañía Samsung, que recoge datos relacionados con la salud de los usuarios. El tratamiento y acceso a los datos se realiza en una plataforma desarrollada por Samsung denominada SAMI[64]. La pulsera se conecta de forma automática con SAMI para subir a la nube todos los datos del usuario. Como anuncia la propia compañía, al tratarse de un dispositivo de construcción modular, puede conectar fácilmente módulos de sensores con nuevas configuraciones. Samsung proporciona ya implementada una funcionalidad de referencia llamada Simsense, que admite múltiples sensores, generando cada uno un flujo de datos único[65]. Y no solo eso, sino que además utiliza un sistema operativo basado en Linux (denominado Tizen[66]) que permite desarrollar nuevos algoritmos para leer y analizar estos datos en tiempo real, o acceder a datos históricos[67] a través de su plataforma de intercambio de datos ARTIK Cloud. ¿Se está informando con este mismo nivel de claridad[68] y obteniendo debidamente el consentimiento para cada uno de estos tratamientos?

---

64 https://developer.samsungsami.io/ [Última consulta: 3 de septiembre de 2018].

65 https://www.simband.io/documentation/simband-documentation/ [Última consulta: 3 de septiembre de 2018].

66 https://www.tizen.org/ [Última consulta: 3 de septiembre de 2018].

67 La propia Google ofrece su API (*application programming interface*) "Google Fit History", que permite "*ejecutar la lectura, inserción, actualización y borrado de datos sobre la forma física*", cuya consideración encaja dentro de la definición de datos relativos a la salud y, en menor medida, datos biométricos. Continúa explicando que los desarrolladores pueden utilizar esta API para leer datos que fueron recogidos por otras aplicaciones, importarlos a Google Fit, actualizarlos, y borrar los datos en la APP que previamente los almacenaba. Se trata de funcionalidad perfectamente conocidas y especificadas, y lo que se ofrece es una interfaz que adelanta y simplifica a los desarrolladores las tareas especificadas: https://www.programmableweb.com/api/google-fit-history [Última consulta: 19 de agosto de 2018]. No es la única, y existen otros ejemplos. Polar AccessLink: "allows you to obtain a direct information sharing link between the Polar ecosystem products such as their health trackers and smart watches and and organization's own data system. Polar provides information on an athlete's sports performance for people's lifestyle, rehabilitation and weight management".

68 Extraído de la página de Simband: "Devices based on the Simband platform can continuously monitor your health and physical activity, as well as educate, coach and

De igual modo, podemos referirnos, por ejemplo, a las smartglasses, que están comenzando a encontrar mercado en los deportes al aire libre que recorren grandes distancias. Pensada para ciclistas o runners, Everysight BEAM (fabricada por la empresa Raptor) anuncia que proporciona información "no intrusiva de acceso fácil"[69]. Sin embargo, como será tónica habitual en el futuro del IoT: "Raptor se conecta a tu Smartphone a través de Bluetooth para que puedas tener siempre acceso a tus emails, textos, agendas y más", además de tener su propio GPS incorporado, Wi-Fi, etc. Convertido en una característica casi indispensable para cualquier wearable, permite tomar: "todas las métricas y sin instalación compleja", para a renglón seguido animar a: "Conecta[r] los sensores para más info, sube tus salidas en bici a go.everysight y comparte en Strava". Cadencia, velocidad, frecuencia cardíaca, o ruta seguida son otros de los datos que recoge y combina. Por último, ofrece compatibilidad con otras aplicaciones, ya que permite importar los entrenamientos de Training Peaks. Tanto la aptitud para recabar datos, como la interconectividad de los dispositivos del futuro, se manifiesta de modo absoluto, y alcanza todo tipo de posibilidades. Capacidad de reconocer objetos y enlazar a dónde comprarlos, leer códigos de barras de productos, hacer fotos o vídeos, lector QR, reconocimiento de texto (OCR)[70], realidad aumentada, emisión de vídeo en directo… El grado de sofisticación alcanzado, el amplio rango de actividades cotidianas en que se aplican, la cantidad y diversidad de datos que pueden recoger, y su vocación de conectividad con otros dispositivos hace de los *wearables* una auténtica mina de datos.

El sector de las básculas inteligentes también ha entrado con fuerza en el mercado, gracias a modelos con precios de entrada muy moderados que comienzan a partir de tan solo 20 euros. Garmin, una de las marcas con mayor peso en el sector de los wearables dedicados a la medición de datos relativos a la salud, presenta una de las básculas más completas. Ofrece la lectura de mútiples valores, tales como: "Índice de masa corporal (IMC), masa muscular, masa ósea, porcentaje de grasa corporal y porcentaje de agua"[71]. A mayor abundamiento, estos datos resultan compatibles y acumulables con los de otros productos de la marca: "Garmin ofrece varios dispositivos compatibles con la medición de tu nivel de actividad o al deporte que prefieras. Ahora,

provide helpful feedback on your wellness. For the first time, you can ask specific health questions and get clear, insightful answers directly from the source: your body".

69 https://everysight.com/es/about-raptor/ [Última consulta: 4 de septiembre de 2018].

70 https://cincodias.elpais.com/cincodias/2017/07/18/gadgets/1500384631_920125.html [Última consulta: 4 de septiembre de 2018].

71 https://www8.garmin.com/manuals/webhelp/indexscale/ES-XM/GUID-CB348359-1E39-491B-86B5-79CB12FB6A8C.html [Última consulta: 4 de septiembre de 2018].

la báscula inteligente Garmin Index ofrece un modo de ver los resultados de tus esfuerzos por mantenerte activo y consultar las estadísticas en Garmin Connect, nuestra comunidad de deporte online".[72] Es más: "Garmin Index cuenta con conexión Wi-Fi, lo que permite sincronizar datos con Garmin Connect. Desde un ordenador o en un dispositivo móvil compatible, Garmin Connect te permite ver tus datos con más detalles y consultar tu progreso respecto a tus objetivos. La báscula inteligente puede reconocer hasta 16 personas y cargar de forma automática sus métricas de composición corporal directamente a sus cuentas de Garmin Connect". En otras palabras: las referidas estadísticas, obtenidas además con una cierta regularidad temporal generando un histórico, son recogidas y combinadas con otras generadas por otros aparatos inteligentes, subidas a la nube, y puestas a disposición en la cuenta personal del usuario. Otras básculas (Withings Smart Body Analyzer) aportan aún más datos, como medición de la frecuencia cardíaca durante el pesaje o análisis continuo de la calidad del aire de la estancia donde se encuentra (temperatura y nivel dióxido de carbono).

Finalmente, para no extendernos en exceso, simplemente a efectos ilustrativos y por ser uno de los dispositivos más populares en el recabamiento de datos biosanitarios, son de obligada mención las pulseras *fitness*. Estos wearables, junto con sus respectivas APPs, recaban datos muy sensibles tales como peso, frecuencia cardíaca, porcentaje de grasa, consumo de calorías y metabolismo basal, presión sanguínea[73], además de otras como medición de las distancias caminadas durante el día, cantidad de horas de sueño y su calidad (diferenciando sueño profundo de sueño ligero)[74], etc. Todo ello es registrado con el tiempo y el lugar en que se llevó a cabo[75]. ¿Cuál es el problema? Que los usuarios facilitan datos sensibles a las compañías que posteriormente sirven para otras múltiples finalidades, como, por ejemplo, explica la compañía Under Armour en su API: "Under Armour Webhooks". Según se revela en la descripción, "permite a los consumidores recibir notificaciones sobre eventos que involucran a sus usuarios, que pueden enviarse a cualquier URL segura mantenida por el consumidor. Algunas características incluyen las más modernas técnicas, optimizadas para obtener detalles sobre la información, impulsada por las experiencias sociales, estimular el rendi-

[72] https://buy.garmin.com/es-ES/ES/p/530464 [Última consulta: 4 de septiembre de 2018].

[73] https://www.programmableweb.com/api/human-utility [Última consulta: 4 de septiembre de 2018].

[74] Por ejemplo, las populares Fitbit: https://help.fitbit.com/articles/es/Help_article/1314 [Última consulta: 4 de septiembre de 2018].

[75] https://www.programmableweb.com/api/google-awareness [Última consulta: 4 de septiembre de 2018].

miento deportivo y más. La plataforma fortalece a los socios y desarrolladores de Under Armour, junto con un conjunto completo de aplicaciones Under Armour: Under Armour Record, MapMyFitness, MapMyRun, MapMyRide, MapMyWalk y MapMyHike"[76].

Esta masa de información recogida y tratada por todos estos elementos del *Internet of Things*, y cuya conectividad individual aumentará con la llegada del 5G, contribuye al fenómeno del Big Data. Sin embargo, se asienta sobre otros elementos prácticos que influyen de manera decisiva en su disponibilidad y existencia. Permisos inadecuados o invasivos para el normal funcionamiento de las APPs, condiciones de privacidad ligadas a condiciones de la contratación, exceso de extensión y falta de claridad en el lenguaje, etc. se combinan con lo ya expuesto.

Todo ello dibuja un fenómeno con identidad propia que no está tratado de forma integral y directa[77] por el RGPD, ya que presenta características únicas que exceden de las previsiones del Reglamento, como bien apunta Beltrán Aguirre[78]. Dicho esto, en la actualidad se están tramitando dos propuestas legislativas a nivel comunitario que pueden afectar de forma decisiva a la regulación de esta materia: el Reglamento e-Privacy[79] y el Reglamento sobre libre circulación de datos no personales[80].

---

[76] https://www.programmableweb.com/api/under-armour-webhooks. "Under Armour Webhooks API allows consumers to receive notifications about events involving their users, that may be sent to any secure URL maintained by the consumer. Some features include; turn-key and state-of-the-art, optimized for insights over information, driven by social experiences, inspires athletic performance and more. The platform powers Under Armour partners and developers, along with a full suite of Under Armour applications: Under Armour Record, MapMyFitness, MapMyRun, MapMyRide, MapMyWalk, and MapMyHike".

[77] Frías, Zoraida / Pérez Martínez, Jorge: "5G networks: Will technology and policy collide?", *Telecommunications Policy*, Nº 42, 2018, pp. 612–621.

[78] Beltrán Aguirre, *op. cit.* p. 122.

[79] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). COM/2017/010 final - 2017/03 (COD). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010 [Última consulta: 5 de septiembre de 2018].

[80] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la libre circulación de datos no personales en la Unión Europea. COM/2017/0495 final - 2017/0228 (COD). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0495 [Última consulta: 5 de septiembre de 2018].

A modo de cierre, puede concluirse que el granjeo incesante de datos es ya imparable[81], se incrementará en el futuro, contiene información muy sensible (datos biosanitarios) y ofrece posibilidades de combinación inabarcables (a continuación observaremos casos reales), ya sean consentidas o producto de filtraciones[82]. Ello forma parte nuclear del fenómeno del Big Data y, a su vez, representa una amenaza real a la protección de datos y a la privacidad, dando lugar a un escenario que intentaremos sintetizar a continuación en pocas líneas. En este sentido, cabe afirmar que, si bien por definición el Big Data se refiere a grandes volúmenes de información, y muchas veces se trata de información no personal, no podemos olvidar que la doctrina[83] viene considerando[84] la anonimización absoluta[85] como algo prácticamente[86] imposible[87], opinión a la que me sumo.

---

81 Considerando 6 RGPD: "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

82 Shu, Xiaokui / Zhang, Jing / Yao, Danfeng / Feng, Daphne, "Fast Detection of Transformed Data Leaks", *IEEE Transactions on Information Forensics and Security*, Vol. XI, Núm. 3 (marzo), 2016, pp. 528-542. P. 528: "Reports show that the number of leaked sensitive data records has grown 10 times in the last 4 years, and it reached a record high of 1.1 billion in 2014".

83 Llàcer Matacás, Mª Rosa / Casado González, María / Buisan Espeleta, Lidia, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Observatori de Bioètica i Dret, Universidad de Barcelona Publicacions i Edicion, 2015, pp. 33 y sgts. Disponible en línea en http://hdl.handle.net/2445/104585. [Última consulta: 2 de agosto de 2018].

84 Cristea Uivaru, Lucia Nicole, "La protección de los datos de carácter sensible en el ámbito europeo: historia clínica digital y big data en salud", tesis doctoral dirigida por Parra Rodríguez, Carmen, Universitat Abat Oliba, Barcelona, 2017, pp. 306-308. Disponible en: http://hdl.handle.net/10803/442972 [Última consulta: 2 de agosto de 2018].

85 Grupo de Trabajo sobre Protección de Datos del artículo 29: "Dictamen 05/2014 sobre técnicas de anonimización", 0829/14/ES, WP216, de 10 de abril de 2014.

86 En un tono algo más crítico Martínez Martínez, Ricard, "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", *Revista Valenciana d'Estudis Autonòmics*, Núm. 62, 2017, pp. 257-259. Disponible en: http://www.transparencia.gva.es/documents/19318353/165265446/RVEA+62+v2-1+Completo.pdf. [Última consulta: 29 de julio de 2018].

87 Diario El Confidencial, edición de 29 de enero de 2015: "Cuatro datos son suficientes para relacionarte con tu tarjeta de crédito", disponible en línea en: http://www.elconfidencial.com/tecnologia/2015-01-29/cuatro-datos-son-suficientes-para-relacionartecon-tu-tarjeta-de-credito_651827/ [Última consulta: 2 de agosto de 2018].

4. El potencial invasivo a través de casos reales. Obtención del consentimiento estratificado o por capas y su viabilidad tecnológica

En efecto, esta problemática es tan real y tan palpable como nos muestran conocidos casos reales. En el año 2006, AOL publicó por error un listado que contenía 20 millones de búsquedas[88] de sus usuarios durante los últimos tres meses, *a priori* sin datos personales, pero con un número asociado a cada búsqueda. Tan solo eso fue suficiente para convertirlos en personas identificadas o identificables. A partir de dicha información, el diario The New York Times[89] consiguió identificar al usuario número 4417749, que resultó ser una ciudadana de 62 años de Lilburn, en el Estado de Georgia, llamada Thelma Arnold, de quien también obtuvieron una imagen que publicaron junto a la noticia (previo consentimiento). El texto de la misma no lo explicita, pero desde su publicación y la aparición de la base de datos, tan solo pudieron transcurrir un máximo de 5 días (desde el 4 de agosto hasta el 9, fecha de la noticia), lo que es una cantidad bastante pequeña de tiempo teniendo en cuenta los recursos de los que se disponían entonces. Lo que sí recoge la noticia es que muchas otras personas fueron identificadas en base a la misma filtración. Este caso, de 2006, es una buena muestra del verdadero potencial de la combinación de datos, incluso pseudonimizados.

Examinemos a continuación otro caso real, en cierto modo paradigmático, que demuestra de forma cruda las vulneraciones de privacidad que se derivan del tratamiento de datos a raíz de su combinación. En 2012, un padre de Minneapolis interpuso una queja en su tienda local de la compañía Target, debido a que su hija, menor de edad, había recibido, a su nombre, un catálogo personalizado y vales de descuento sobre productos para el embarazo (incluyendo ropa de bebé y cunas)[90]. Ya resultando bastante llamativo y fuera de lugar recibir publicidad personalizada sobre algo que atañe tanto a la esfera de la intimidad como es un embarazo, este caso era aún más grave tratándose de una menor. El problema es que, mediante esta

---

88 Ramasastry, Anita, "Privacy and Search Engine Data: A Recent AOL Research Project Has Perilous Consequences for Subscribers", *Law Technology*, Washington, Vol. XXXIX, Núm. 4, 2006, pp. 7-9.

89 https://www.nytimes.com/2006/08/09/technology/09iht-aol.2431152.html [Última consulta: 9 de agosto de 2018].

90 https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp; https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4b5ce3346668 [Última consulta: 2 de septiembre de 2018].

publicidad, Target había revelado al padre el verdadero estado de gravidez en que se encontraba la menor, que había decidido mantenerlo en secreto, en una demostración de cuán invasivo puede realmente llegar a ser el fenómeno objeto de estudio. La combinación de datos tiene, en efecto, tal potencial[91]. Nos encontramos de facto ante una afectación de la intimidad que lleva a pensar que se ha traspasado una línea de no retorno, pues la disponibilidad y capacidad para la recombinación de toda la información que generamos, incluida la biosanitaria, es tecnológicamente susceptible de crear situaciones como las de los casos reales expuestos. En este caso, con el agravante de que la información atañe al núcleo duro de la intimidad[92], con un potencial excepcional, y con efectos que se expanden a todo tipo de circunstancias.

Esta situación no siempre viene dada por la combinación de datos a través de cesiones de datos, que constituyen una operación con cierta complejidad jurídico-tecnológica, sino que, como ya expusimos con anterioridad, las filtraciones de información y brechas de ciberseguridad son aprovechadas para obtener bases de datos y perfiles más o menos completos que, posteriormente, son vendidos en el mercado negro[93].

Otras veces se deben a fallos (en ocasiones, muy convenientes) en la programación de las propias aplicaciones en relación con las condiciones o con el consentimiento recabado. Por ejemplo, al cierre de este artículo, Associated Press reveló la noticia de que Google almacena localizaciones a pesar de haber desactivado la opción principal (aparentemente, habría que desactivar adicionalmente la pestaña "actividad web")[94]. Tras ello, la

---

91 Shen, Yushi / Li Yale / Wu, Ling / Liu, Shaofeng / Wen, Qian, "Big Data overview", *Big Data: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications,* Information Resources Management Association (vvaa), Information Science Reference, Hershey, Pensilvania, Estados Unidos, 2016, pp. 15-16.

92 Crawford, Kate / Schultz, Jason, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review* Vol. LV, Núm. .1, p. 93-128. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/bclr55&i=94 [Última consulta: 2 de septiembre de 2018]. P. 94: "Personal harms emerge from the inappropriate inclusion and predictive analysis of an individual's personal data without their knowledge or express consent. For example, in 2012, a well-publicized New York Times article revealed that the retail chain Target had used data mining techniques to predict which female customers were pregnant, even if they had not yet announced it publicly. This activity resulted in the unauthorized disclosure of personal information to marketers".

93 Hutchings, Alice / Holt, Thomas J., "The online stolen data market: disruption and intervention approaches", *Global Crime*, Vol. XVIII, Núm. 1, 2017, pp. 11-30. Disponible en: https://www.tandfonline.com/doi/pdf/10.1080/17440572.2016.1197123 [Última consulta: 2 de septiembre de 2018].

94 https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not [Última consulta: 14 de septiembre de 2018].

compañía estadounidense no ha cambiado el comportamiento del software, sino la redacción de sus condiciones[95]. Este no es sino un caso más de los tratamientos que las compañías llevan a cabo con un consentimiento que no se ha obtenido para tal finalidad o, en su caso, no se ha especificado de manera clara y explícita, sino mediante un lenguaje complejo, eufemístico, en ocasiones subterfugioso o, sencillamente, enrevesado. ¿Alcanza esta clase de comportamiento el alto estándar de información clara y transparente que exige el RGPD, máxime en datos biosanitarios?[96]

Como ya introdujimos con anterioridad, podrían existir dudas importantes en la forma en que se presenta la información para la obtención del consentimiento. Un ejemplo de modelo funcional sobre consentimiento estratificado según finalidad, son las *cookies*, que desde la entrada en vigor del RGPD han venido presentando información individualizada y la posibilidad de distinguir y aceptar o rechazar cada uno de los tratamientos (estratificado o "por capas")[97], distinguiendo, por ejemplo, cookies obligatorias, técnicas, de preferencias, personalización, mediciones, monitorización de uso y publicidad.

Dado que se ha demostrado su viabilidad tecnológica, y su mejor encaje jurídico en el marco del nuevo RGPD, no existen motivos por los que no se pueda replicar el esquema en *wearables* y aplicaciones que gestionan datos biosanitarios, máxime cuando, a diferencia de las *cookies*, estos datos son especialmente sensibles. En otras palabras: no existen motivos que impidan que se informe y recabe el consentimiento específico para cada finalidad, como exige el Reglamento. En este sentido, nótese que uno de los grandes problemas que hay que tener en cuenta en esta materia, además, es que los datos que se obtienen por las compañías creadoras de estos *gadgets* son muchos y muy variados, con un potencial vulnerador de la intimidad muy serio. Resulta muy indicativo que en agosto de este año, el Ministerio de Defensa de Estados Unidos, a través del Pentágono, haya prohibido con carácter general

---

95 https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211 [Última consulta: 14 de septiembre de 2018].

96 Teijeiro Lillo, María Eugenia, "La práctica profesional a través de dispositivos móviles electrónicos", *Salud electrónica. Perspectiva y realidad,* Pérez Gálvez, Juan Francisco (Coord.), Tirant lo Blanch, Valencia, 2017, p. 133.

97 Noain-Sánchez, Amaya, "'Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication & Ethics in Society*, Vol. XIV, Núm. 2, 2016, pp. 124-138.

las APPs de *fitness* y las pulseras de ejercicio (como las aquí anteriormente expuestas) a los militares desplegados en zonas operacionales[98].

Recordemos asimismo en esta misma línea, y en conexión con las filtraciones de datos, cómo a principios de año la aplicación de ejercicio Strava reveló (a través de mapas de calor con miles de millones de puntos de GPS tomados de las mediciones a los soldados) las posiciones de efectivos militares en la frontera entre Corea del Norte y del Sur, las ubicaciones de bases secretas del ejército de los Estados Unidos, y las rutas de entrenamiento de los soldados[99].

En definitiva, lo que trata de significarse, es que nos encontramos ante grandes cantidades de datos muy concretos y detallados, y que además son altamente sensibles. Si conectamos esta realidad con hechos como las filtraciones de datos, brechas de seguridad, la existencia de un mercado negro de los datos, la realidad de la explotación del Big Data *in-house*[100] [101], el creciente potencial de granjeo de datos gracias a la tecnología 5G e IoT (*Internet of Things*), y los peligros que ya hemos expuesto sobre la combinación de datos, encontramos una situación que, a pesar de ser delicada, es ya irreversible.

5. Conclusiones

Recapitulemos los datos relativos a la salud que captan y tratan algunos de los diferentes dispositivos inteligentes, *wearables*, y exponentes de la *Internet of Things* que hemos mencionado: pulso cardíaco, presión arterial, horas de sueño, calidad del sueño, peso, masa corporal, masa ósea, masa muscular, porcentaje de agua, porcentaje de grasa corporal o visceral, actividad física, consumo de calorías, metabolismo basal, ubicación, distancias recorridas, huella dactilar, reconocimiento facial, etc. Todos estos datos se transmiten, intercambian y combinan entre sí con otros dispositivos, ofreciendo resultados que son registrados periódicamente (por ejemplo, cada día, dando lugar a seguimiento, estadísticas e informes muy completos) que además son

98 http://www.elmundo.es/tecnologia/2018/08/14/5b6de9d3e5fdea8e7a8b4586.html [Última consulta: 14 de septiembre de 2018].

99 http://www.elmundo.es/tecnologia/2018/01/29/5a6eef30e2704ef57c8b45a8.html [Última consulta: 14 de septiembre de 2018].

100 Gregory, Adrian, "Data governance -- Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability", *Journal of Direct, Data and Digital Marketing Practice*; Vol. XII, Núm. 3 (enero-marzo), 2011, pp. 230-248.

101 https://www.elperiodico.com/es/economia/20180910/bbva-presidente-datos-7027824 [Última consulta: 10 de septiembre de 2018].

exportables a teléfonos inteligentes, tablets, ordenadores, e incluso la nube, asignados a una cuenta personal.

¿Se está obteniendo el consentimiento de forma adecuada para estos tratamientos? ¿Son claras y transparentes las condiciones? ¿Se está informando de manera explícita y separada para cada finalidad como exige el considerando 32? Dado que, de base, todo tratamiento de datos relativos a la salud está prohibido, salvo que medie consentimiento expreso y por escrito del interesado para cada finalidad (art. 9.1), sin la cuidada obtención del mismo para cada una de ellas, podríamos estar ante algunos casos de tratamientos ilícitos. La sensibilidad de los datos recogidos, la cantidad de los mismos, y su periodicidad, son una información muy para los datos para aseguradoras, compañías de medicina privada, bancos, y otros muchos agentes de mercado que pueden valerse de la misma, constituyendo una fuente de riqueza[102].

Es inútil ir contra el signo de los tiempos, y cuestiones como el Big Data, la existencia de mercados de datos, los diversos modelos de negocio[103] arbolados en torno a ellos, la creciente capacidad de captura y procesamiento de datos personales, etc., son parte de la idiosincrasia del siglo XXI, de igual modo que el telar mecánico, la máquina de vapor o la electricidad lo fueron anteriormente en siglos precedentes. Como con gran acierto dicen (y desarrollan brillantemente) De Lecuona Ramírez y Villalobos-Quesada: "El cambio de paradigma hacia una economía guiada por el dato para mejorar la toma de decisiones en la sociedad digital, potencia el uso y la mercantilización de conjuntos de datos personales, ente los cuales los datos de salud son de especial interés por el valor intrínseco que posee, y por el que puede adquirir mediante su explotación a escala Big Data"[104].

Ahora bien, no podemos caer ni en la ingenuidad de ignorar la existencia de esta realidad, ni en la inocencia de que, gracias al RGPD y la LOPDGDD, nuestros datos están guardados a buen recaudo y a salvo. Considero que de base existe una falta de información e insuficiente pedagogía para con el público general, que adolece de una falta de concienciación sobre por qué existe la protección de datos y qué bienes jurídicos pretende salvaguardar. La

---

[102] Zeng, Jing / Glaister, Keith W., "Value creation from big data: Looking inside the black box", *Strategic Organization*, Vol. XVI, Núm. 2, 2018, pp. 105-140.

[103] Escribano Cañas, Blanca, "*Dos proyectos de Reglamento europeos mantienen en vilo a la llamada 'economía de los datos' de la Unión"*, Actualidad Jurídica Aranzadi, Núm. 937/2018. BIB 2018\6127

[104] De Lecuona Ramírez, Itziar / Villalobos-Quesada, María, *ob. cit.* Versión Proview.

relevancia de ello aumenta cuando los datos que se tratan son especialmente sensibles y pertenecen a la esfera de la intimidad, como son los datos relativos a la salud y biométricos.

A la luz de los antecedentes en materia de combinación de datos, puestos de manifiesto mediante algunos casos prácticos, podemos decir que ya hemos experimentado que la acumulación y cruce son perfectamente posibles, conduciendo a resultados indeseables. Esto, unido a que existen robos de datos, filtraciones de estos, se producen fallos de ciberseguridad, etc., trae como consecuencia la existencia de mercados para los datos, gracias a los cuales puede reunirse mucha información que conduzca a personas físicas individuales. Existe la posibilidad real de comprar datos, cruzarlos, obtener perfiles, y aplicarlos a individuos.

Considero esta cuestión preocupante, porque se recoge muchísima información y su capacidad para afectar de forma directa a la intimidad, e incluso, al libre desarrollo de la personalidad, se me hace cada vez más real y palpable. Hasta ahora, los informes específicos sobre los aprovechamientos de la información biosanitaria en base a datos de 2015, revelan que el uso que se ha venido dando ha sido secundario. La popularización de los *wearables* en estos últimos años, que está promoviendo la salida de los datos relativos a la salud fuera del clásico esquema prestacional hacia uno más comercial, contribuirá a aprovechamientos más sofisticados por los agentes del mercado (así como a combinaciones más complejas), con la diferencia de que, en este caso, hablamos de datos sensibles, con una gran capacidad invasiva en la esfera más íntima del individuo.

Adicionalmente, observo un potencial desequilibrio contractual de información y de conocimiento a favor de las empresas frente a los individuos, que ahonda en la distancia abismal de fuerzas y que, sin límites, será cada vez más grande[105]. Esto no son sino más medios adicionales en el conocimiento del negocio, tendencias, formas de uso, etc. Se trata de una hiperespecialización y conocimiento muy profundo y pormenorizado de la parte fuerte del contrato (empresario) para su explotación y maximización de beneficios frente a los consumidores y usuarios, generando una asimetría de fuerzas evidente. No hay incentivos económicos para las empresas en "empoderar al usuario"[106]. Solo acciones legislativas pueden mejorar sus derechos y

[105] *Ibídem*.

[106] Ilten, Carla / Guagnin, Daniel / Hempel Leon, "Privacy self-regulation through awareness? A Critical Investigation into the Market Structure of the Security Field", European Data Protection: In Good Health?, Gutwirth, Serge / Leenes, Ronald / De Hert, Paul / Poullet, Yves

su posición negocial, como bien se ha demostrado con el RGPD. En esta materia tan sensible, puede producirse una afectación al derecho a la salud (y, en su caso, a la vida), sobre todo en países donde la preponderancia del sistema sanitario privado es superior al público, con capacidad para generar potenciales discriminaciones "en nombre de la investigación científica, la excelencia y la innovación"[107].

En este trabajo se ha dedicado especial interés a exponer casos reales y aplicaciones vigentes, así como dispositivos existentes, disponibles para su compra. Y ello porque quiere demostrarse que las problemáticas expuestas, que surgen del tratamiento de datos sanitarios, no son visiones retrógradas ni distópicas. Son problemas reales como lo son los casos, las *APPs*, y los *wearables* citados. Es ya un problema del presente inmediato, pero, evidentemente a medida que transcurran los años y se acumulen más datos, más vulnerables podrán ser las personas. Al fin y al cabo, los individuos son generadores Big Data en materia sanitaria, pero resulta complicado que puedan por sí solos beneficiarse de él directamente.

Mi conclusión es que es necesario afrontar esta nueva realidad desde una doble perspectiva. Por un lado, debe incidirse en la concienciación ciudadana, lo que requiere de un esfuerzo divulgativo y pedagógico importante. Por el otro, es necesario abordar una mejora en la transparencia, claridad de la información y estratificación del consentimiento por parte de las compañías, debido a su viabilidad tecnológica y su mejor adecuación al marco regulatorio. Sentado lo anterior, cabría afirmar que, si el individuo tiene interés en proteger su privacidad, debe considerar la posibilidad de no adoptar determinadas tecnologías. No puede afirmarse que la información que se recoge por *apps* y *smart devices* se encuentre garantizada, a pesar de que una normativa garantista como es el nuevo RGPD ya está contribuyendo a mejorar los estándares de protección de la información y de ciberseguridad.

(eds.), Springer, 2012. P. 246: "We have argued that the market structures in the security field are obscure to the extent that no incentives for self-regulation are perceived by the actors involved. Security actors are clearly interested in making a profit and do not have sufficient intrinsic motivation to kick-start self-regulation". Demand for more attention to privacy would have to be forced upon these actors, but no one currently articulates this demand within the market".

[107] De Lecuona Ramírez, Itziar / Villalobos-Quesada, María, *op. cit*. Versión de Proview.

6. Bibliografía

Barral Viñals, Inmaculada, "Datos relativos a la salud e historia clínica: La confidencialidad de los datos médicos", *Protección de datos personales en la sociedad de la información y la vigilancia,* Llácer Matacás, María Rosa (Coord.), Ed. La Ley, Las Rozas, Madrid, España, 2011.

Beltrán Aguirre, Juan Luis, "Tratamiento de datos personales de salud: incidencia del Reglamento General de Protección de Datos", *Salud electrónica. Perspectiva y realidad,* Pérez Gálvez, Juan Francisco (Dir.), Tirant lo Blanch, Valencia, España, 2017.

Crawford, Kate / Schultz, Jason, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review* Vol. LV, Núm. 1, 2014.

Cristea Uivaru, Lucia Nicole, "La protección de los datos de carácter sensible en el ámbito europeo: historia clínica digital y big data en salud", tesis doctoral dirigida por Parra Rodríguez, Carmen, Universitat Abat Oliba, Barcelona, España, 2017.

Daranas, Manuel, "Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana", *Boletín de Jurisprudencia Constitucional*, Dirección de Estudios y Documentación del Congreso de los Diputados, Tomo IV (Jurisprudencia Constitucional Extranjera), Núm. 33, Madrid, España, 1984.

Davara Fernández de Marcos, Isabel, *Hacia la estandarización de protección de datos personales,* Ed. La Ley, Las Rozas, Madrid, España, 2011.

De Franceschi, Alberto, *European contract law and the digital single market*, Intersentia, Cambridge, Reino Unido, 2016.

De Lecuona Ramírez, Itziar / Villalobos-Quesada, María, "El valor y el precio de los datos personales de salud en la sociedad digital", *El cuerpo diseminado: estatuto, uso y disposición de los biomateriales humanos,* García Manrique, Ricardo (Coord.), Aranzadi, Cizur Menor, España, 2018.

Elvy, Stacy-Ann, "Commodifying consumer data in the era of the internet of things", *Boston College Law Review*; Vol. LIX, Núm. 2, 2018.

Escribano Cañas, Blanca, "Dos proyectos de Reglamento europeos mantienen en vilo a la llamada 'economía de los datos' de la Unión", *Actualidad Jurídica Aranzadi*, Núm. 937, 2018.

Fernández Agis, Domingo, "Humanismo, posthumanismo e identidad humana", *Ius et Sciencia: Revista Electrónica de Derecho y Ciencia*, Vol. IV, Núm. 1, 2018.

Fernández López, Juan Manuel, "Principio de consentimiento: Título II. Principios de la Protección de Datos. Artículo 6", *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, Troncoso Reigada, Antonio (Coord.), Thompson Civitas, Madrid, España, 2010.

Frías, Zoraida / Pérez Martínez, Jorge, "5G networks: Will technology and policy collide?", *Telecommunications Policy*, Núm. 42, 2018.

Goozner, Merril, "Do you know your healthcare credit score?", *Modern Healthcare*, Vol. XLVI, Núm. 23 (junio), 2016.

Gregory, Adrian, "Data governance -- Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability", *Journal of Direct, Data and Digital Marketing Practice*; Vol. XII, Núm. 3 (enero-marzo), 2011.

Grupo de Trabajo sobre Protección de Datos del artículo 29: "Dictamen 05/2014 sobre técnicas de anonimización", 0829/14/ES, WP216, de 10 de abril de 2014.

Guama Morales, Sonia Carolina, "Estudio comparativo de métodos existentes para integrar la información estructurada y no estructurada de una industria enfocado en la generación de conocimiento, desde la perspectiva de una solución integral de Big Data", repositorio digital de postgrados (Maestría en Gerencia de Sistemas y Tecnologías de la Información) de la Universidad de las Américas, Chile, 2015.

Hilbert, Martin / López, Priscila, "The World's Technological Capacity to Store, Communicate, and Compute Information", *Science*, Vol. CCCXXXII, Núm. 6025 (abril), 2011.

Hutchings, Alice / Holt, Thomas J., "The online stolen data market: disruption and intervention approaches", *Global Crime*, Vol. XVIII, Núm. 1, 2017.

Ilten, Carla / Guagnin, Daniel / Hempel Leon, "Privacy self-regulation through awareness? A Critical Investigation into the Market Structure of the Security Field", *European Data Protection: In Good Health?,* Gutwirth, Serge / Leenes, Ronald / De Hert, Paul / Poullet, Yves (eds.), Springer, 2012.

Kelly, Eileen P. / Erickson, G. Scott, "Legal and privacy issues surrounding customer databases and e-merchant bankruptcies: reflections on Toysmart.com", *Industrial Management & Data Systems*; Vol. CIV, Núm. 3/4, 2004.

Lemstra, Wolter, "Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implication", *Telecommunications Policy,* Vol. XLII, 2018.

Llàcer Matacás, Mª Rosa / Casado González, María / Buisan Espeleta, Lidia, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Observatori de Bioètica i Dret, Universidad de Barcelona Publicacions i Edicion, Barcelona, España, 2015.

Luzak, Joasia, "Is All Fair in War Against Unhealthy and Unsustainable Lifestyles? The Right to Privacy vs. Modern Technology in Consumer Contracts", *The Constitutional Dimension of Contract Law: A comparative perspective*, Siliquini-Cinelli, Luca / Hutchison, Andrew (Eds.), Springer International Publishing, Cham, Suiza, 2017.

Martínez Martínez, Ricard, "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", *Revista Valenciana d'Estudis Autonòmics*, Núm. 62, 2017.

Noain-Sánchez, Amaya, "'Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication & Ethics in Society*, Vol. XIV, Núm. 2, 2016.

Ochagavías Colás, Juan Ignacio, "Una panorámica de las nuevas tecnologías aplicadas al ámbito de la salud a propósito del m-Health y sus interacciones jurídicas", *DS: Derecho y salud*, Vol. XXVI, Núm. Extra 1 (Ejemplar dedicado a:

XXV Congreso 2016: El avance de las Ciencias de la Salud y las incertidumbres del Derecho), 2016.

Parliament House of Commons. Science and Technology Committee, *Responsible Use of Data. Fourth Report of Session 2014-15*, The Stationery Office Limited, Londres, Reino Unido, 2015.

Ramasastry, Anita, "Privacy and Search Engine Data: A Recent AOL Research Project Has Perilous Consequences for Subscribers", *Law Technology*, Washington, Vol. XXXIX, Núm. 4 (octubre-diciembre), 2006.

Ramón Fernández, Francisca, "La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico", *Métodos de Información*, Vol. VIII, Núm. 14, 2017.

Rebollo Delgado, Lucrecio, *Vida privada y protección de datos en la Unión Europea*, Ed. Dykinson, Madrid, España, 2008.

Rita Palattella, Maria et ál., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models", *IEEE Journal on Selected Areas in Communications*, Vol. XXXIV, Núm. 3 (marzo), 2016.

Shen, Yushi / Li Yale / Wu, Ling / Liu, Shaofeng / Wen, Qian, "Big Data overview", *Big Data: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications,* Information Resources Management Association (vvaa), Information Science Reference, Hershey, Pensilvania, Estados Unidos, 2016.

Shu, Xiaokui / Zhang, Jing / Yao, Danfeng / Feng, Daphne, "Fast Detection of Transformed Data Leaks" *IEEE Transactions on Information Forensics and Security*, Vol. XI, Núm. 3 (marzo), 2016.

Teijeiro Lillo, María Eugenia, "La práctica profesional a través de dispositivos móviles electrónicos", *Salud electrónica. Perspectiva y realidad,* Pérez Gálvez, Juan Francisco (Coord.), Tirant lo Blanch, Valencia, España, 2017.

Vázquez de Castro, Eduardo, "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* Núm. 46, 2018.

Zeng, Jing / Glaister, Keith W., "Value creation from big data: Looking inside the black box", *Strategic Organization*, Vol. XVI, Núm. 2, 2018.

Participative consent: Beyond broad and dynamic consent for health big data resources*

Consentimiento participativo: Más allá de los consentimientos genérico y dinámico para las iniciativas de salud de datos masivos

PhD. María Villalobos-Quesada

Researcher, Bioethics and Law Observatory - University of Barcelona (Barcelona, Spain)

DOI: 10.14679/1146

Sumario / Summary: 1. Introduction. 2. The current situation of personal data. 3. Big data resources for health. 4. Consent for health big data resources. 4.1. Specification of objectives. 4.2. Towards a model of representative consent 4.3. Granting access to for-profit entities. 5. Conclusions.

Resumen / Abstract: Hoy en día participamos de una sociedad del conocimiento donde gran parte de nuestras vidas ha sido digitalizada. Esta transformación ha afectado productos y servicios y ha cambiado nuestras actividades profesionales, académicas y personales. La magnitud de la digitalización de nuestra sociedad ha permitido generar y almacenar datos de (casi) todo. A través de la investigación e innovación, esta información nos brinda grandes oportunidades para mejorar nuestra salud y los sistemas de salud de los que depende. El presente estudio está interesado en los proyectos de salud de datos masivos que utilizan este tipo de información personal y que son establecidos como facilitadores al servicio de la investigación e innovación. Puesto que llevan diferentes nombres, como 'biobancos' o 'proyectos genoma', se les referirá en este artículo como 'proyectos de salud de datos masivos' o 'iniciativas'. El objetivo principal de este estudio es identificar

* Article received on October 15, 2018 and accepted for publication June 9, 2019.
Corresponding authors: María Villalobos-Quesada (mvillalobos@ub.edu).

un modelo de consentimiento que le permita a estos proyectos funcionar de acuerdo con los valores de la UE, respetar los derechos humanos fundamentales y satisfacer las expectativas de los participantes, de los titulares de los datos y de la sociedad en general. Actualmente en la UE, los modelos de consentimiento utilizados para estas iniciativas responden a la transformación de los modelos socioeconómicos, a los cambios en las políticas nacionales y de la UE (incluyendo el nuevo Reglamento General de Protección de Datos), a los avances científicos y tecnológicos y al abandono de la idea de anonimización absoluta. Desde el punto de vista de los ciudadanos, el consentimiento debe responder a sus expectativas con respecto a su salud, bienestar, servicios sanitarios, ciencia y tecnología. Puesto que el consentimiento se ve influenciado por múltiples factores, diferentes modelos se proponen para proyectos de datos masivos en salud y hay un interés constante en mejorarlos. Hoy en día, los modelos de consentimiento utilizados en proyectos de salud de datos masivos se han alejado del modelo tradicionalmente utilizado en la investigación clínica o biomédica. En su lugar se adoptan modelos de consentimiento genérico o presunto.

Este análisis está en línea con la tendencia actual que considera el modelo tradicional de consentimiento informado inadecuado para los proyectos de salud de datos masivos. Va más allá y hace hincapié que el cambio a modelos de consentimiento genérico o presunto es un cambio positivo, pero insuficiente. El principal objetivo de este trabajo es hacer un llamado para que las iniciativas de datos masivos en salud incluyan sistemas de gobernanza representativos. Estos sistemas deben facilitar los medios para que participantes, titulares de los datos y ciudadanos puedan codirigir las operaciones de estos proyectos, comunicar su voluntad y mantener cierto nivel de control sobre sus datos personales a través del tiempo. En otras palabras, es necesario implementar estructuras de gobernanza que permitan extender el concepto tradicional de consentimiento, entendido como el ejercicio de la autonomía de aquellos implicados. Esto requiere que el consentimiento sea modificable (que pueda cambiar a través del tiempo) y participativo. El éxito de iniciativas basadas en estos modelos de consentimiento dependerá en gran medida de la confianza de los ciudadanos, participantes y titulares de los datos, para lo cual debe establecerse un proceso de diálogo permanente y participación pública como parte integral de los sistemas de gobernanza de los proyectos de salud de datos masivos.

Nowadays, we participate in a knowledge-based society where a large part of our lives has been digitalised. Products, services, and professional, academic and personal activities have turned digital and with that change, it became possible to record and collect data about (almost) everything. Through research and innovation, this information has offered great opportunities to improve health and the health systems it depends on. The present study is interested in initiatives that use this kind of personal information, specifically, big data initiatives that serve as resources to support research and innovation, such as 'biobanks' or 'genome projects'. They will be further referred in this paper as 'health big data resources' or 'initiatives'. The main goal of this work is to identify a model of consent that would allow these initiatives to align with EU values, respect fundamental rights and meet the expectations of participants, data subjects and society. In the EU, consent responds to the different socioeconomic contexts, the national and EU policy (including the General Data Protection Regulation), and to the abandonment of the idea of absolute

anonymisation. From the point of view of citizens, consent should respond to their expectations regarding health, well-being, health systems, science and technology. Because it is shaped by multiple factors, there are different models of consent used in health big data resources and there is a constant interest in improving them. The current tendency is that consent has shifted away from the model used in traditional clinical or biomedical research. Instead, big data resources are adopting models of broad or assumed consent.

This analysis supports the current general idea that the traditional concept of informed consent is insufficient for supporting health big data resources. Moreover, it stresses that it is insufficient to simply move towards models of broad or assumed consent. The main purpose of this analysis is to show that health big data initiatives should aim towards a model of consent based on a representative governance system. Through this system, participants, data subjects and society will be able to influence the initiative's operations, communicate their will and retain a certain level of control over their personal data and the activities of the resource. In other words, it is necessary to strive for mechanisms to extend the traditional concept of consent through governance which would enable the exercise of autonomy of those implicated. Therefore, consent must become not only modifiable (in the sense that it should be allowed to change through time), but participative. For these models of consent to be successful, they must be grounded in a solid relationship of trust with participants, data subjects and society in general. Consequently, it is necessary to establish a permanent process of dialogue and public engagement with the goal of informing, shaping and directing the governance systems of big data resources for health.

Palabras clave / Keywords:

Salud / Datos masivos / Consentimiento participativo / Consentimiento informado / Consentimiento genérico / Consentimiento presunto / Gobernanza / Sociedad del conocimiento / Biobancos / Proyectos genoma / Unión Europea.

Health / Big data / Participative consent / Informed consent / Broad consent / Assumed consent / Governance / Knowledge-based society / Biobanks / Genome projects / European Union.

1. Introduction

The current situation of consent in health big data initiatives can only be successfully analysed if placed in the context of an extensively digitalised society and economy. Here, private and public parties massively collect and use personal data from very different sources. Specifically regarding public data, including health-related information, its use is explicitly promoted by the European Union (EU)[1] and it has given rise to public and private initiatives

[1] European Commission, "A Digital Single Market Strategy for Europe", *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* Brussels, Belgium, 2015, pp.

to reuse it. The present study is a response to the ethical issues raised by the use of personal data in health big data initiatives which are promoted as resources for research and innovation, such as 'biobanks' or 'genome projects'. They will be further referred in this paper as 'health big data resources' or 'initiatives'. Some examples of such initiatives, not all of them currently active, are: PADRIS and VISC+ in Catalonia, Generation Scotland, UK Biobank, Qatar Genome Programme, Estonian Genome Project, Saudi Human Genome Project and the International Cancer Genome Consortium. Though relevant, for-profit initiatives such as 23&Me, which reuses costumers' data for collaborative research[2], is beyond the scope of this research.

Usually, health big data resources do not follow for-profit schemes, instead they are based on arguments such as the common good and solidarity. Not surprisingly, these initiatives are heterogeneous. They are led by different kinds of organisations, such as governments, non-profit organisations or private parties. Furthermore, they make use of medical information, use other sources to infer health-related information, or use a combination of both. Medical information is unanimously considered sensitive, but health-related information has not been traditionally considered as such. This situation poses important practical and regulatory challenges.

Since consent continues to raise many questions in the context of these initiatives, the present study focuses on the models of consent used. There have been meaningful developments in this regard. Models of consent have changed according to new scientific and technological advancements, such as interoperability, connectivity, technological portability, and massive digitalisation of the health systems and social life in general. Furthermore, consent has responded to the socioeconomic conditions, to policy changes at national and EU levels, to citizens' expectations regarding health, science and technology, and to the abandonment of the idea of absolute anonymisation. Additionally, the supply and demand of health services and other products and services related to health and wellbeing have also transformed the approach to consent.

Resources that support research and innovation were initially conceived as banks of tissues and human samples. Nowadays, big data resources have

1-20. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN [Last accessed: 20 July 2019].

[2] 23andMe reports that since 2010 it has published 139 scientific papers and collaborates with academic centres, industry and non-profits. More information available at: https://www.23andme.com/publications/ [Last accessed: 20 July 2019].

used the foundation of those banks and acquired more diverse human samples and more data to complement the traditional clinical information. For example, they incorporated new sources of personal data that is used to derive health information, referred here as 'health-related data'. All this information needs to be considered personal and sensitive, because of the purpose of processing. There is nothing original with considering health-related information sensitive. It is just the logical evolution of the category of sensitive data, according to the current technological and scientific developments. Given the importance of this data, consent is a central tool to protect the fundamental rights of those involved and to guarantee that individuals will not be victims of abuse or misuse of their personal information.

This work discusses decisive factors related to the model of consent applied to health big data resources in the EU. What can we learn about the models of consent used by the current ongoing big data resources? Most importantly, what can we learn from the issues, challenges and barriers that these initiatives have faced? It is not the purpose of this paper to offer a detailed examination of legal and practical requirements necessary to articulate an adequate consent. The goal of the present study is to identify and discuss key factors related to the models of consent used in health big data resources, initiatives based on sensitive personal information. In this way, it aims to serve as a guide when deciding how to structure this type of initiatives.

2. The current situation of personal data

At the beginning of the present century, the European Council pointed EU's way forward: 'to become the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion'[3]. According to the Council, globalisation and the knowledge-based economy, were affecting 'every aspect of people's lives'. As a result, the EU was 'confronted' with the challenge to respond to those changes, in a way that is consistent with EU values and concepts of society. The identification of the so-called 'EU values' and 'concepts of society' is a perpetual task. Relevant efforts have made to construct frameworks to assist ethical evaluation; for example, the work of

[3] European Council, "Lisbon European Council 23 and 24 March 2000. Presidency Conclusions", Lisbon, Portugal, 2000. Available at: http://www.europarl.europa.eu/summits/lis1_en.htm#6 [Last accessed: 20 July 2019].

the European Group on Ethics in Science and New Technologies (EGE), an independent advisor to the European Commission[4].

The concept of a knowledge-based economy can be understood in the wider context of a 'knowledge-based' or 'knowledge-driven' society. The European Commission defines it as 'a society whose processes and practices are based on the production, distribution and use of knowledge'[5]. That implies that data, information and knowledge have been turned into wealth and power. Hand in hand with that transformation, the human capacity of recording, acquiring and using data has increased at an incredible rate. For example, it has been estimated that by 2020 each person[6] will generate data equivalent to the capacity of 200 CDs per day. That means that each person will generate 1.7MB per second[7].

Nowadays the use of massive amounts of information has been incorporated into a field known as big data. Although massive but unanalysed data is considered to have very low intrinsic value, it has a huge potential to inform decision-making in virtually any terrain. When dealing with massive amounts of information, knowledge is gained through a process which involves mathematic algorithms, data analytics or data processing, which reveals correlations or patterns that are not necessarily evident from the raw data. This process is commonly known as big data to knowledge[8].

Although a definition of big data depends greatly on the author, a suitable working definition is the following. Big data can be defined as the acquisition, management and use of massive digital data, which depends on

---

4 More information about the EGE, including its reports and declarations, is available at: https://ec.europa.eu/research/ege/index.cfm [Last accessed: 20 July 2019].

5 European Commission, "Glossary", Electronic Platform for Adult Learning in Europe, 2018. Available at: https://ec.europa.eu/epale/en/glossary/knowledge-based-society [Last accessed: 20 July 2019].

6 World's population numbered nearly 7.6 billion as of mid-2017 and it is projected to be 8.6 billion by 2030.
UN, "Key Findings and Advance Tables, Key Findings and Advance Tables", ESA/P/WP/248, Department of Economic and Social Affairs Population Division, New York, 2017, pp. 1-46. Available at: https://population.un.org/wpp/Publications/Files/WPP2017_KeyFindings.pdf [Last accessed: 20 July 2019].

7 Domo, "Data Never Sleeps 6.0", 2018, pp. 1-7. Available at: https://www.domo.com/learn/data-never-sleeps-6 [Last accessed: 20 July 2019].

8 Margolis, Ronald / Derr, Leslie / Dunn, Michelle *et ál.,* "The National Institutes of Health's Big Data to Knowledge (BD2K) Initiative: Capitalizing on Biomedical Big Data", *Journal of the American Medical Informatics Association,* No. 6, Vol. 21, 2014, pp. 957-958. doi:10.1136/amiajnl-2014-002974.

software and hardware components. Big data, as a phenomenon of the digital society, has greatly relied on scientific and technological advances in areas such as electronic and computer engineering, informatics, mathematics and physics[9]. Depending on their specific characteristics and capabilities, systems may be able to report results and recommendations to human controllers, or systems may act upon results and take decisions automatically. They may have different degrees of human supervision, intervention and feedback, which is commonly referred to as 'independence' or 'autonomy'. Actually, the term 'autonomous systems' is currently in use to refer to systems that can learn to perform tasks by themselves, which typically require intelligence when carried out by a human. Autonomous systems can have a physical scaffold, such as high-tech robotic systems, or be purely digital, such as intelligent software. However, it is important to clarify that the term 'autonomous' in this context does not refer to autonomy in the moral sense[10].

Under the momentum marked by the Lisbon strategy, the EU has built knowledge infrastructures, enhanced innovation, and modernised social welfare and education systems.[3] Furthermore, the EU embraced the construction of a data economy and a 'single data market'.[1] Innovation is driven from many fronts, notably from science and technology, and it is in the hands of public or private organisations, or both. Universities have become centres of innovation, and private-public and university-business models thrive with the support of the EU[11]. Both sides take advantage of these partnerships. On one hand, the academic centres, which find a way to face the increasing cuts and funding limitations. On the other hand, the private sector, which participates in an aggressive and highly competitive market[12]. An example of the blending of digitalisation and innovation is the digitalisation of the public health systems, which allows the reuse of data for secondary purposes. Reutilisation, according to the European Commission is encouraged, and can

---

9 De Lecuona, Itziar / Villalobos-Quesada, María, "European Perspectives on Big Data Applied to Health: The Case of Biobanks and Human Databases", *Developing World Bioethics,* No. 3, Vol. 18, 2018, pp. 291-298. doi:10.1111/dewb.12208.

10 EGE, "Artificial Intelligence, Robotics and 'Autonomous' Systems", European Group on Ethics in Science and New Technologies, European Commission, Luxemburg, pp. 1-24. doi:10.2777/786515.

11 Council of the eu, "Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, of 26 November 2009 on developing the role of education in a fully-functioning knowledge triangle", 2009. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42009X1212%2801%29 [Last accessed: 20 July 2019].

12 ankrah, Samuel / Al-Tabbaa, Omar, "Universities-Industry Collaboration: A Systematic Review", *Scandinavian Journal of Management*, 2015, pp. 1-22. doi:10.1016/j.scaman.2015.02.003.

be carried out in the context of commercial and non-commercial activities, independently of the initial purpose of collection[13],[14].

The new digital socioeconomic model has raised many questions and has generated tangible challenges in the EU and elsewhere. For example, in the UK the Information Commissioner's Office fines amounted more than £4M in 2017[15], the Catalan Data Protection Authority reported that sanctions amounted €58.000 the same year[16] and the European Data Protection Supervisor received the highest amount of complaints during the period 2015-2017 (143, 173 and 141 complaints respectively)[17]. Furthermore, several personal-data scandals received aggressive media coverage, turning privacy and data protection into a public topic. Some examples are the cases of TalkTalk[18], Facebook[19], Equifax[20], Securus[21] and Cambridge Analytica and Facebook[22].

---

[13] European Commission, "European legislation on the re-use of public sector information", Digital Single Market, Policy, 2013. Available at: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information [Last accessed: 20 July 2019].

[14] European Commission, "Towards a Thriving Data-Driven Economy", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 2014, pp. 1-12. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/towards-thriving-data-driven-economy [Last accessed: 20 July 2019].

[15] Archer, Joseph, "Data protection fines hit record last year as GDPR deadline looms", *The Telegraph*. Available at: https://www.telegraph.co.uk/technology/2018/05/22/data-protection-fines-hit-record-last-year-gdpr-deadline-looms/ [Last accessed: 20 July 2019].

[16] Acpd, "Memòria 2017", Catalan Data Protection Authority (Autoritat Catalana de Protecció de Dades), Government of Catalonia, 2017, pp. 1-127, in Catalan. Available at: http://apdcat.gencat.cat/web/.content/01-autoritat/memoria_anual/documents/MEMORIA-2017_APDCAT-final.pdf [Last accessed: 20 July 2019].

[17] European Data Protection Supervisor, "Annual Report 2016", European Union, Luxemburg, 2017, pp. 1-71. doi:10.2804/807674.

[18] Ismail, Nick, "7 key lessons from TalkTalk's data breach", *Information Age,* 25 October 2016. Available at: http://www.information-age.com/7-key-lessons-talktalks-data-breach-123462859/ [Last accessed: 20 July 2019].

[19] Gómez, Rosario G., "Spanish data protection agency slaps Facebook with €1.2 million fine", *El país,* 11 September 2017. Available at: https://elpais.com/elpais/2017/09/11/inenglish/1505143866_490497.html [Accessed 20 July 2019].

[20] Fung, Brian, "Equifax's massive 2017 data breach keeps getting worse", *The Washington Post*, 1 March 2018. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/ [Last accessed: 20 July 2019].

[21] Barret, Brian, "A Location-Sharing Disaster Shows How Exposed You Really Are", *Wired*, 19 May 2018. Available at: https://www.wired.com/story/locationsmart-securus-location-data-privacy/ [Last accessed: 20 July 2019].

[22] Rosenberg, Matthew / Confessore, Nicholas / Cadwalladr, Carole, "How Trump Consultants Exploited the Facebook Data of Millions", *The New York Times*, 17 March 2018.

In view of these challenges, the European Parliament called for the protection of fundamental rights and privacy in the context of big data. This call concerns directly the big data resources for health, because they are initiatives that store and share great volumes of personal sensitive information. The Parliament also recognised that the line between sensitive and non-sensitive data is becoming increasingly difficult to determine, because the growing capabilities of big data allow the inference of sensitive information from data that is not traditionally considered as such[23]. Equally, this is a challenge that has to be addressed by health big data projects. A possible solution is to consider personal information according to the processing context, the objective of collection and analysis, and not strictly according to the nature of the data. For example, the recently adopted General Data Protection Regulation (GDPR)[24] can be interpreted in this way. That means that if data is used for 'sensitive purposes', or used to derive sensitive information, the one responsible for the data (the data controller) must comply with the requirements to process sensitive data ('special categories of personal data', according to the language of the GDPR)[25].

The GDPR represents an opportunity to harmonise EU data privacy laws and introduces changes at the level of organisations in order to protect data privacy. This is of great importance in the context of research and innovation, and it has an impact on health big data resources and the projects that seek access to the information they hold. Furthermore, the Regulation articulates

---

Available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [Last accessed: 20 July 2019].

[23] European Parliament, "Report on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement", Plenary Sitting, Committee on Civil Liberties, Justice and Home Affairs, rapporteur: Ana Gomes, 2017. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0044+0+DOC+PDF+V0//EN [Last accessed: 20 July 2019].

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[25] According to the GDPR, *op. cit*. note 24, sensitive data is be defined as data which is relevant to fundamental rights and freedoms in such a way that data processing potentially generate important risks. It includes the 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

responsibility mechanisms for data controllers[26] and processors[27], independently of the localisation of their head offices. It also approaches citizens by recognising their rights to their own personal data and by empowering them. Furthermore, it aims to protect citizens from misuse, abuse and data breaches. The GDPR is of special relevance, because it limits business models that thrive on personal information and were previously largely unregulated. Health is an attractive and lucrative sector that strongly attracts the investment of the private sector, which would be affected by the Regulation. Although it is too soon to assess the whole impact of the GDPR, it immediately increased the reports of data breaches[28] and caused a general response from data controllers who needed to comply with the new data security and privacy measures, and adjust the conditions of the agreements of users or consent.

A peculiarity of the GDPR relevant for health big data resources is that it gives scientific research obligations, but also special freedoms. The Regulation requires scientific research to protect the rights and freedoms of data subjects and to respect the principle of data minimisation. Additionally, anonymisation or pseudonymisation should be carried out when possible. However, it gives scientific research special privileges[29]. Scientific research is an exception to the principles of purpose limitation and storage limitation, and to the rights to be forgotten and to object. Equally, it is one of the exceptions to the prohibition to process special categories of personal data, and to the obligation to inform data subjects about processing of their personal data when that is impossible or when it involves a disproportionate effort. This means that health big data resources will enjoy these freedoms. However, it also means that harmonised codes of conduct are necessary to govern the activities of these resources and the research they support. Consent, also post-GDPR, will continue to have a central role in defining and communicating to the participants and data subjects their rights. In the cases when consent is not considered 'necessary', other mechanisms will have to ensure that interests and fundamental rights

[26] According to the GDPR, *op. cit*. note 24, controller 'means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

[27] According to the GDPR, *op. cit*. note 24, processor 'means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

[28] Rashid, Fahmida Y., "Data Breach Reports Spike After GDPR", *Decipher,* Duo Security, 30 July 2018. Available at: https://duo.com/decipher/data-breach-reports-spike-after-gdpr-goes-into-effect [Last accessed: 20 July 2019].

[29] GDPR, *op. cit*. note 24, Articles 5, 9, 14, 17, 21 and 89, and Preamble Recitals 33, 50, 52, 62, 65, 156.

of data subjects are respected. The central proposal of this work of extending the concept of consent to governance mechanisms, as it will be discussed later, will be a key tool to address this issue.

3. Big data resources for health

Recently, health has been shifting away from the negative definition of 'absence of disease or infirmity', towards a concept of health understood as 'a state of complete physical, mental and social well-being'[30]. Importantly, it aims to perpetuate a healthy state and prevent disease. That approach to health ushers the incorporation of information from varied sources in order to determine, evaluate and understand health. Some examples of these sources of information are levels of daily activity, sport, physiological readings, and preferences and habits such as diet, alcohol consumption, smoking and interaction with other people. Recording and quantifying these types of activities or conditions have been enabled by mobile technologies and devices, which form part of the Internet of Things (IoT)[31]. Furthermore, science and technology have facilitated the use of new sources of information; for example, genetic data (genomics), profiles of gene expression (transcriptomics), metabolism (proteomics and metabolomics), and many other 'omics' fields[32].

Big data is an incredible tool that allows the incorporation of all this information in the context of health. Through big data analyses, disconnected and heterogeneous data can be incorporated into individual and collective profiles. These can be examined over time or compared to other profiles in order to answer particular questions; for example, about longevity, the transition health to disease, disease progression, remission, response to treatment, relapse, metastasis in cancer, death and effects of heritable factors or the environment. According to EU authorities, big data is a key tool to

[30] WHO, "Constitution of the World Health Organization", Basic Documents, Forty-Fifth Edition, Supplement, 2006, pp. 1-18. Available at: http://www.who.int/governance/eb/who_constitution_en.pdf [Last accessed: 20 July 2019].

[31] Dey, Nilanjan / Ashour, S. Amira / Bhatt, Chintan, "Internet of Things Driven Connected Healthcare", *Internet of Things and Big Data Technologies for Next Generation Healthcare*, Studies in Big Data 23, Dey, Nilanjan / Ashour, S. Amira / Bhatt, Chintan (Ed.), Cham, Switzerland, Springer International Publishing AG, 2017, pp. 3-12. doi:10.1007/978-3-319-49736-5.

[32] The suffix 'omics' is used to indicate scientific fields based on high-throughput (large scale) technologies, which entails to a big extent the automation of processes in order to acquire and analyse massive amounts of information in parallel.

improve patient outcomes and evidence-based healthcare decision-making[33]. Furthermore, together with eHealth and mHealth[34], it is considered to have the potential to improve the health of EU citizens and successfully face the future challenges posed to the healthcare system by an aging population, increased citizens' mobility and patients' expectations.

4. Consent for health big data resources

Informed consent designed for traditional clinical or biomedical research is based on the assumptions that there is a clinician-patient relationship and that there is a known and well-established research objective. An individual decides to take part in research programmes based on a process of informed consent where there is an opportunity to discuss the implications of taking part with the clinician or the promoter of the research project. However, none of these assumptions necessarily apply to health big data resources. Databases that collect and manage massive data represent such high investment and are considered to have such great potential that, although established with a goal in mind, it is often impossible to narrow the purposes of the research they aim to support. Additionally, the rapid advancement of science and technology enable the use of novel sources of information and gives rise to new applications; for example, the IoT and the new information and communication technologies (ICT) that are applied to health.

Seeking informed consent to participate in clinical or biomedical research is also based on the premise that participants' data can be anonymised, which has now been proven impossible in the context of big data. In today's information society, anonymisation or absolute protection of privacy is

[33] Stril, Arthur / Dheur, Stéphanie / Hansroul, Nicolas *et ál.,* "Big Data in Healthcare", European Health Parliament, 2015, pp. 1-12. Available at: http://www.healthparliament.eu/wp-content/uploads/2017/09/Big-data-in-health-care.pdf [Last accessed: 20 July 2019].

[34] eHealth is defined by the European Commission as 'using digital tools and services for health', it includes: electronic health records, telemedicine, ePrescription and mHealth. mHealth is defined by the WHO as 'medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices'.
Şener, Yasemin / Albertino, Giulia / Bénié, Kolia *et ál.*, "Electronic/Mobile Health", European Health Parliament, 2015, pp. 1-20. Available at: http://www.healthparliament.eu/wp-content/uploads/2017/09/Electronic_mobile-health.pdf [Last accessed: 20 July 2019].

impossible to ensure. The former has been shown by numerous reports[35],[36]. Specifically, some point out that individuals can be singled out using very simple demographics[37], genomic[38],[39] or gene expression data[40]. An example of this change of paradigm is the GDPR, which considers pseudonymisation[41] a technical measure to ensure data protection.

Finally, it cannot be overemphasised that big data resources for health are based on highly sensitive information; for example, medical records, health information or other data that can be used to infer health or disease factors. Although the last one is not traditionally considered sensitive, when used in the context of health, it should be considered as such. The model of consent for health big data resources needs to find a middle ground between the protection of data subjects and the support given to a high number and a wide range of research projects. Such consent depends greatly on the level of trust of participants and data subjects, and on building the proper mechanisms to maintain that trust through time. Consent also determines much of the contact and relationship between the resource and participants or data subjects. Meaning that consent dictates the access to the decision-making processes, which stresses even further the importance of choosing an appropriate model of consent.

---

35 Check Hayden, Erika, "Privacy Protections: The Genome Hacker", *Nature News*, 24 April 2013. doi:10.1038/496411a.

36 Check Hayden, Erika, "Privacy Loophole Found in Genetic Databases", *Nature News*, 17 January 2013. doi:10.1038/493451a.

37 Sweeney, Latanya, "Simple Demographics Often Identify People Uniquely", *Carnegie Mellon University*, Data Privacy Working Paper 3, 2000, pp. 1-34. Available at: https://dataprivacylab.org/projects/identifiability/paper1.pdf [Last accessed: 20 July 2019].

38 Gymrek, Melissa / Mcguire, Amy L. / Golan, David / et al., "Identifying Personal Genomes by Surname Inference", *Science,* Vol. 321, 2013, pp. 321-324. doi:10.1126/science.1229566.

39 Sweeney, Latanya / Abu, Akua / Winn, Julia, "Identifying Participants in the Personal Genome Project by Name", *Cornell University Library*, 2013, pp. 1-4. arXiv:1304.7605 [cs.CY]

40 Schadt, Eric E / Woo, Sangsoon / Hao Ke, "Bayesian method to predict individual SNP genotypes from gene expression data", *Nature Genetics*, No. 5, Vol. 44, 2012, pp. 603-608. doi:10.1038/ng.2248.

41 According to the GDPR, op. cit. note 24, pseudonymisation 'means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

4.1. Specification of objectives

Currently, in the context of health big data resources and as a response to the lack of specific research purposes, informed consent is usually broad or assumed, and it is accompanied by an opt-out option. For example, the UK Biobank is a non-profit initiative in hands of a registered charity. It recruited half a million participants using a broad consent model assisted by a representation mechanism, and established that it will facilitate the contents of the resource to carry out research that is defined as 'health-related', '*bona fide*' and of 'public interest'[42]. It has approved research in areas as diverse as physical activity, life-style behaviours, mental health, sleep, cancer, hearing and diabetes[43].

The adoption of broad or assumed consent is also a response to the great number of research projects which these resources seek to support. Again, the UK Biobank has to date 1,463 applications at various stages of adjudication, including 1003 applications of research projects focused on genetics or phenotyping.[43] In this context, it is easy to understand why the specific consent is impractical, laborious and unachievable in practice. It becomes unrealistic to demand from participants to re-consent to such great number of heterogeneous research proposals. Furthermore, re-consent would be administratively difficult and would change the data and samples available for each study, making comparative studies difficult or impossible. For these reasons, broad consent is an adequate option for health big data resources. However, there must be a real effort to formulate and communicate a clear profile for participants to understand the general objectives of the resource and the objectives of those who will access their personal information.

There is another model of consent generally applied to nation-wide health big data resources, the assumed consent. For example, the Catalan government is directing the Public Data Analysis for Health Research and Innovation Program (PADRIS in Catalan)[44], which should currently be in the

---

[42] Uk Biobank Coordinating Centre, "Access Procedures: Application and Review Procedures for Access to the UK Biobank Resource", Version 1.0, 2011. Available at: https://www.ukbiobank.ac.uk/wp-content/uploads/2012/09/Access-Procedures-2011.pdf [Last accessed: 20 July 2019].

[43] Uk Biobank, "Approved Research Summary". Available at: http://www.ukbiobank.ac.uk/approved-research/ [Last accessed: 20 July 2019].

[44] AQuAS, "Data Analytics for Health Research and Innovation Public Program –PADRIS–" (Programa Públic d'Analítica de Dades per a la Recerca i la Innovació en Salut a Catalunya –PADRIS–) Agency for Health Quality and Assessment of Catalonia (Agència de Qualitat i Avaluació Sanitàries de Catalunya), Department of Health, Barcelona, 2017,

phase of full operation and evaluation, but no reports are available since 2017. The initiative is based on the creation of a unified Catalan health database from primary healthcare and hospital data held by the Catalan health system. According to available reports, the government will use the personal information of citizens based on assumed consent complemented with an opt-out option. PADRIS will grant access to research projects which are aligned with: the EU research and innovation strategies, the Catalonian Strategic Plan for Health, Research and Innovation[45], the Spanish strategies implemented under the Carlos III Health Institute[46], and the priorities established by the Catalan Health Plan[47]. To set the definition of the research goals of a national initiative in these kinds of terms is inadequate if the goal is to reach and communicate with the public. Furthermore, the initiative's website[48] does not specify further information. However, it is stated that PADRIS will ensure the benefit for the citizens and the health system.

It is also of the foremost importance for the resources to understand the expectations of participants, data subjects and society. In order to ensure a climate of enduring trust, it is key to limit data sharing only to research projects well-accepted by participants, data subjects and the society they belong to, projects which do not challenge social values and interests. Here, the research field, the techniques applied and the intended final applications must be taken into account. It must be avoided to grant access to research

---

pp. 1-37, in Catalan. Available at: http://aquas.gencat.cat/web/.content/minisite/aquas/publicacions/2017/Programa_analitica_dades_PADRIS_aquas2017.pdf [Last accessed: 20 July 2019].

45 Government of Catalonia, "PERIS 2016-2020. The Strategic Plan for Health, Research and Innovation", Ministry of Health, Directorate-General for Health Research and Innovation, Barcelona, 2016, pp. 1-61. Available at: http://salutweb.gencat.cat/ca/ambits_actuacio/linies_dactuacio/recerca/peris-2016-2020/ [Last accessed: 20 July 2019].

46 Government of Spain, "Spanish Strategy for Science, Technology and Innovation 2013-2020" (Estrategia Española de Ciencia y Tecnología y de Innovación 2013-2020), Ministry of Economy and Competitiveness, 2013, pp. 1-42, in Spanish. Available at: http://www.ciencia.gob.es/stfls/MICINN/Investigacion/FICHEROS/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf [Last accessed: 20 July 2019].

47 Government of Catalonia, "Marking Milestones for 2020. The Health Objectives of the Catalan Health Plan 2016-2020" (Marcant Fites per al 2020. Els Objectius de Salut del Pla de Salut de Catalunya 2016-2020), Ministry of Health, 2017, in Catalan. Available at: http://salutweb.gencat.cat/web/.content/_departament/pla-de-salut/Pla-de-salut-2016-2020/fites-2020.pdf [Last accessed: 20 July 2019].

48 AQuAS, "Public Data Analysis for Health Research and Innovation Program (PADRIS) (Programa d'analítica de dades per a la recerca i la innovació en salut)", Department of Health-Agency for Health Quality and Assessment of Catalonia, last update unknown, in Catalan. Available at: http://aquas.gencat.cat/ca/ambits/analitica-dades/padris/ [Last accessed: 20 July 2019].

projects that fall outside the consent agreed upon (in the cases of broad consent) or the goals communicated to the public (in the case of assumed and broad consent), or when research projects cause social division or disapproval. This is a matter of foremost importance in the case of nation-wide resources, because these initiatives are usually based on assumed consent and depend more strongly on information campaigns that target the general public at a national level. If a resource suspects that a particular line of research is socially controversial, the most progressive approach is to take a step towards society, data subjects and participants, and explore their opinions. Otherwise, the resource should simply avoid supporting this type of research. A good example is the situation generated by the adoption of the UK Human Fertilisation and Embryology Act in 2008[49], which regulated the use of human tissue for somatic-cell nuclear transfers (hSCNT). Because these techniques divided public opinion, Generation Scotland, a resource of human biological samples and data available for medical research, decided to take a clear precautionary position and request explicit consent from donors for projects that involved the creation of human or admixed embryos using this technique[50].

How can administrators of big data resources for health be truly informed about social opinions, when science, research and innovation advance at an incredible rate? And when science, technology and society influence each other constantly? Although some information can be derived from the consent or recruitment process, these actions do not apply to all initiatives, for example when assumed consent is used. Here I would like to propose that an important part of the solution lies in a governance system that allows the involvement of participants, data subjects and society, and will effectively take into account their views. Such approach is in line with current bioethical discussions. For example, last year during the presentation of the document 'Genome Editing and Human Reproduction' of the Nuffield Council on Bioethics[51], a recurrent point was the importance of giving the general public

[49] Human Fertilisation and Embryology Act 2008. An Act to amend the Human Fertilisation and Embryology Act 1990 and the Surrogacy Arrangements Act 1985; to make provision about the persons who in certain circumstances are to be treated in law as the parents of a child; and for connected purposes.

[50] Jones, David A. / Mackellar, Calum, "Consent for Biobank Tissue in Somatic-Cell Nuclear Transfer", *The Lancet,* Vol. 374, 2009, pp. 861-863. doi:10.1016/S0140-6736(09)61609-3.

[51] Nuffield Council on Bioethics, "Genome Editing and Human Reproduction", London, United Kingdom, 2018, pp. 1-183. Available at: http://nuffieldbioethics.org/wp-content/uploads/Genome-editing-and-human-reproduction-FINAL-website.pdf [Last accessed: 20 July 2019].
More information about the conference available at: http://nuffieldbioethics.org/news/2018/launch-event-genome-editing-human-reproduction-ethical-issues [Last accessed: 20 July 2019].

its rightful place in bioethics, to 'respect the public's intuition' and to have 'humility' to listen and to be informed by public discussions[52]. An effective way to do this is through governance systems that function as a continuation of the consent or authorisation given by participants and data subjects. It is important to stress that it is not enough to simply include members of the civil society in the organisational structure of the resource. In parallel, public participation and engagement should become part of a permanent, integral and transversal part of big data initiatives for health. These tasks should be under the responsibility of a permanent body or commission. Equally important, public participation and engagement in the fields of science and technology need to lie in the core of the national agendas, which should allocate enough budget to conduct this line of research at a national level.

4.2. Towards a model of representative consent

Generally, health big data resources are not short-term initiatives. On the contrary, they have the goal of maintaining themselves through time. Long-term objectives allow for the collection of data from a large number of people at multiple points in time, increasing the amounts of information available. The more data available, the more valuable these resources become. Furthermore, some of the information gathered by these resources, such as genomic data, does not lose its value through time. On the contrary, it is considered to have very high predictable value. This data is relevant, now and in the future, to the individual from whom it originates, to present and future relatives, and to 'unrelated' people who share a particular genetic profile. Although genomic data is the most common high-throughput data, other types of 'omics' data should be considered to have similar potential; for example, epigenetic and gene expression data.

For these reasons, it is an unsuitable and deficient measure for initiatives that control health information, or any other type of data in the context of health, to establish consent as a static act. In other words, taking into account that the information held by health big data resources can easily affect the fundamental rights of those implicated, it is insufficient to give participants and data subjects a single opportunity to request and receive information, and to decide the conditions to share and allow others to use their personal information. Relying uniquely on offering an opt-out option is a minimalistic approach that puts in danger the trust of the public, participants and data subjects, that risks the success of the initiative, and that ignores the input

[52] Based on the interventions of Siobhán O'Sullivan and Jackie Leach Scully, and the corresponding discussions.

of those most implicated. Strictly speaking, initiatives based on broad or assumed consent could make this mistake.

The opt-out option that is offered in the case of resources based on broad and assumed consent should be invariably offered, working as an ultimate mechanism to safeguard the interest of individuals. It is important to not forget that from a practical point of view, it 'shall be as easy to withdraw as to give consent'[53]. However, if opting-out is seen as a right, or at least a way to enact the right to decide over ones' own information, individuals need to be aware that their data is being used, by whom and to which ends. Even though the goals of health big data resources are broad, that does not mean that participants and data subjects cannot be given enough information to understand the global objectives of the resource. Otherwise, the opt-out option is only a deception. Furthermore, opting-out has limitations associated with the traceability of samples, which is associated with the particular scientific experiments and the generation of data, where sometimes individual data is not possible to disengage from the processed data as a whole. Given these limitations, opting-out should not be the only option available for subjects to participate in the governance and decision-making of big data initiatives in which they agree, or at least do not refuse, to take part.

Given the challenges that health big data resources face when dealing with consent, it has become apparent that assumed and broad consent does not fulfil all expectations (of participants, society and of the managers of the resources). Consequently, other types of consent have been proposed. A popular model is the dynamic consent, which is seen as a two-way communication system between participants and researchers based on transparency and respect [54,55]. This model of consent is seen as a possible way to increase trust and participants' engagement[56]. In general, it aims to create an online platform to bridge participants with the controllers of their data and the researchers. However, it is a model of consent that needs significant resources

[53] GDPR, *op. cit*. note 24, Article 7, Conditions for consent.

[54] Stein, Dorit T / Terry, Sharon, "Reforming biobank consent policy: a necessary move away from broad consent toward dynamic consent", *Genetic Testing and Molecular Biomarkers*, No. 12, Vol. 17, 2013, pp. 855-856. doi:10.1089/gtmb.2013.1550.

[55] Teare, Harriet J.A. / Morrison, Michael / Whitley, Edgar A. *et ál.,* "Towards 'Engagement 2.0': Insights from a study of dynamic consent with biobank participants", *Digital Health*, Vol. 1, 2015, pp. 1-13. doi:10.1177/2055207615605644.

[56] Williams, Hawys / Spencer, Karen / Sanders, Caroline *et ál.,* "Dynamic consent: a possible solution to improve patient confidence and trust in how electronic patient records are used in medical research", *JMIR medical informatics*, No. 1, Vol. *3*, 2015, e3 pp. 1-7. doi:10.2196/medinform.3525.

and requires participants to feel comfortable with the platform. To build such 'one-fits-all' platform is a challenge in itself. It will most likely be successful when participants are homogeneous, but not otherwise. For example, younger people consider online platforms more accessible than older people. Others have pointed out other downsides of the dynamic consent, such as the risk of generating therapeutic misconception and individualizing the review of research projects[57].

The main point behind the criticisms of broad and assumed consent is that there is very poor input of the participants and data subjects, who are too far from the decision-making process and the functioning of the resources. These types of consent do not generally facilitate involvement and participation. That creates a gap where resources can drift away from the interests of participants, data subjects and society. Great part of these issues can be overcome if consent becomes modifiable and participative. This could improve the functioning, the acceptance and support given to health big data resources. Furthermore, it would bring resources closer to participants, data subjects and society. That would make the resources receptive to the perspectives and knowledge of those implicated and will facilitate the respect of their rights and interests. Consent should become modifiable in the sense that participants and data subjects must have accessible mechanisms available to adjust their participation and contribution to the resource according to what they consider to be correct, valid, desirable or proportional. These mechanisms should be available as long as the initiative remains active. Participative in the sense that consent should become more than the act of signing a form. It should be extended to the governance systems, which would enable participants and data subjects to influence the activities of the resources along their operations.

There are two useful ways to understand the mechanisms that facilitate a modifiable and participative consent. The first way is to consider them part of the governance systems. However, it is valuable in theory and in practice if those systems are regarded as an extension of the practice of consent, systems that facilitate the right of participants and data subjects to voice their will and preferences and to effectively decide the role they want to play in health big data resources. In other words, they can be regarded as mechanisms designed to enact the autonomy of data subjects and participants. The members of the commissions that decide about the objectives of the health

[57] Steinsbekk, Kristin S. / Myskja, Bjørn K. / Solberg, Berge, "Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?", *European Journal of Human Genetics*, Vol. 21, 2013, pp. 897-902. doi:10.1038/ejhg.2012.282.

big data resources and the research projects they support, should understand that their role is not different from that of representative democratic systems. They have been chosen to participate in those commissions to represent the will and the interests of a group of people, the participants, the data subjects and society in general. Of course they have obligations with the resource itself, with its good functioning, but these resources exist because individuals are willing to share their information to achieve a greater good. Therefore, their first obligation should be to honour the participants' and data subjects' interests, and to protect their rights. They should represent the society as a whole and since this is a difficult task, it is key to reach out to participants, data subjects and the general public. An obvious approach is to include members of the public, participants and representatives of interest groups in the governance system. Although it is a good approach, it should not be forgotten that these members will have their own backgrounds and particular interests, to such an extent that some of them have actively looked forward to participating in these resources. Therefore, that cannot be the only solution; what brings me to the following approach.

A second way of regarding the mechanisms that enable a modifiable and participative consent is to consider them as a permanent communication process. For this purpose, it is necessary to ensure the establishment of the appropriate communication channels. To maintain such channels costs time and money. Resources should see these costs as an investment and should take them into account as part of the permanent costs of operation. Because of the current generalised internet access, the easiest option is to have a website and an online form available for participants and the general public to ask questions or make requests. An email address could also serve a similar purpose. Although in principle, online written communication should be an efficient communication channel, it should not be the only one. Telephone access should be possible; if necessary, specific consultation hours could be offered. Finally, the value of offering direct physical access cannot be forgotten. For example, open days are a powerful means to enact transparency and build trust. My personal experience in a scientific research institution taught me that the interaction between scientist with the general public and participants works two ways. Scientists recognise the goal they work for, they can give a face to those who they want to help. This contact helps researchers to understand the bigger picture. It inspires science in a very different, more human way. On the other end, participants and the general public can see through the eyes of scientists, can put on their lab coats and sit at their benches, where experiments are performed. It breaks that wall

built by having knowledge generated in specific and closed environments, the scientific research centres.

A possible disadvantage of a participative and modifiable consent is that it could trigger constant modifications and limitations to the use of personal data. In order to ensure a stable relationship with data subjects and participants, it is necessary to guarantee an exceptional initial process of communication and engagement. This is particularly relevant in the cases of broad and assumed consent, which aim to overcome the unrealistic requirement to obtain specific consent to approve a great number of research projects. The abandonment consent for specific research objectives should not necessarily result in poor communication with data subjects and participants. On the contrary, it requires foresight and planning to define the goals of the resource. It also requires to construct conceptual categories to reflect the research projects that the resource will support, since it will be impossible to name each research project. Some examples of categories that could be used are: cancer research, rare diseases, metabolic diseases, diabetes, disabilities, infectious diseases, genetic diseases, neglected diseases, reproductive health etc. Another option is to keep the objectives really broad and offer the option to specify exceptions, for example: health-related research or research of public interest. In this second case, it would be necessary to explain possible exceptions, what brings us back to the categories of research.

During the initial process of communication and engagement it is useful to differentiate between individuals with previous knowledge and individuals with limited or no previous knowledge. The first ones are, for example, part of interest groups, have participated or know someone that has participated in similar initiatives, or have professional profiles related to health, biomedicine or scientific research. The second ones are very heterogeneous, but in general they are less familiar with health big data resources. Because of that, they need to be invited, to be offered relevant information about the resource and its objectives in order to engage and communicate efficiently with them. The initial process of communication and engagement is typically carried out during the enrolment process, which would normally conclude with a written agreement. The process of acquiring informed consent offers the perfect opportunity to ensure that consent is truly informed and voluntary, and that the participant has been listened to and guided through the technical and practical information about the resource. To provide the right and relevant information that each participant needs will continue to be at the core of the process of obtaining consent. Members of society are heterogeneous; for example, they have different interests, levels of education, age, soci-

oeconomical contexts and life experiences. There cannot be one uniform solution to obtaining consent. That is why the idea that consent is obtained by 'informing' participants should be abandoned. The process needs to be regarded as a communication process, in order to be open to a two-way dialogue. Furthermore, the process of enrolment offers the right conditions to corroborate that the participant is aware of the channels to interact with the resource. Public campaigns will definitely be a tool to increase the general knowledge about the resources and will make the process of consent easier and more efficient because the general population will already have background information. In the case of assumed consent, these goals will have to be met by the public engagement campaigns and the establishment of accessible channels communication.

In parallel, articulated efforts to communicate and seek feedback from the general public must be in place. Public engagement activities and public reporting should be regarded as permanent requirements for the resource's operations. This is important because resources which reuse health and health-related personal information in the context of big data become the administrators of highly sensitive data which is being shared with third parties. Participants, data subjects and society have expectations that need to be clear to those managing big data resources. To forsake those could cause the participants' and public's rejection and generate distrust, which could damage not only the specific resource but the relationship of society with science and technology. If consent is assumed, the public engagement process has to guarantee all the above.

The great challenge of making sure that the objectives of health big data resources are aligned with the values, interests, and expectations of the public, is that these change overtime, stressing the relevance of a permanent two-way dialogue. Data subjects should be informed that their data is being used, by whom and for what means. Given the nature of health big data resources, data subjects will not receive specific information of each research project that may use their data, but they should have a good idea of the kind of research projects that the resource will support. As an act of transparency, the resource should regularly release public reports about its activities. For example, releasing yearly reports and keeping an updated website with information about outreach, research activities and press releases. It is also relevant that anyone interested can have access to the resource governance frameworks, code of conduct, ethical guidelines, and information about the internal structure and procedures.

It should also be considered that there may be reasonable grounds for family members, cultural or ethnic groups, or members of society to request the removal of personal information from a participant who is not alive or not able to make independent decisions anymore. In this case, there must be a body prepared to determine the potential or actual damage caused, determine the risks and benefits, and weigh the rights and interests at stake. Death or lack of competency should not irrevocably surrender personal information to a particular resource. This position is in line with policies to maintain a relationship of trust with participants, data subjects and society.

Although there is definitely discussion about it, there is evidence to believe that, in the EU, there is a general climate of trust regarding science and technology[58],[59],[60]. This is a view further supported by national reports. For example, more than half of Spanish and British citizens consider that the benefits brought by science and technology outweigh the risks, 81% of UK citizens consider that science makes their lives easier and 90% consider that scientists make valuable contributions; while in Spain, medical doctors, scientists and professors are the most valued professionals[61],[62].

Despite these good signs, we should not be overconfident. The relationship of Europeans with science and technology is not straightforward and there are seemingly contradictory views. Europeans want to be consulted about decisions regarding science and technology but feel poorly informed (only 11% of respondents considered themselves to be 'very well informed') and think that scientists should be better at communicating

---

58 European Commission, "Science and Technology Special Eurobarometer 340", Wave 73.1, TNS Opinion & Social, 2010, pp. 1-158. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_340_en.pdf [Last accessed: 20 July 2019].

59 European Commission, "Special Eurobarometer 419. Public Perceptions of Science, Research and Innovation", Wave EB81.5, TNS Opinion & Social, 2014, pp.1-100. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_419_en.pdf [Last accessed: 20 July 2019].

60 European Commission, "Public Opinion on Future Innovations, Science and Technology. Aggregate Report", Qualitative study, TNS Qual+, 2015, pp. 1-93. doi:10.2777/691455.

61 Fecyt, "Social Perception of Science and Technology 2016" (Percepción Social de la Ciencia y la Tecnología 2016), Spanish Foundation for Science and Technology, Ministry of Economy, Industry and Competitivity, Government of Spain, 2017, pp. 1-376, in Spanish. Available at: https://www.fecyt.es/es/publicacion/percepcion-social-de-la-ciencia-y-la-tecnologia-en-espana-2016 [Last accessed: 20 July 2019].

62 Castell, Sarah / Charlton, Anne / Clemence, Michael / *et al.*, "Public Attitudes to Science 2014", Main Report, Ipsos Mori, Social Research Institute, Department for Business, Innovation and Skills, 2015, pp. 1-194. Available at: https://www.ipsos.com/sites/default/files/migrations/en-uk/files/Assets/Docs/Polls/pas-2014-main-report.pdf [Last accessed: 20 July 2019].

with the public. However, the great majority (91% of respondents) never or rarely participate in public debates or meetings. This situation indicates that there are unaddressed barriers that stand between the public and those who carry out public engagement activities. It seems that the public believes that it has the right to be taken into account in decision-making, but does not access the venues or the available means through which it can be effectively incorporated in the governance systems. An appropriate design of consent should help to bring down these barriers through the establishment of channels for participants, data subjects and society to enact their autonomy, truly participating in the decision-making of health big data resources that affect and involve them.

4.3. Granting access to for-profit entities

It is important for health big data resources to define and communicate the role of the private sector and the conditions for giving access to projects or entities which pursue for-profit objectives. Those should be communicated through the process of consent and public engagement. Interestingly, some relevant resources, including Generation Scotland and the UK Biobank, are open to the private sector and recognise that commercial applications may stem from the use of the resources. Both of them recruited participants and applied broad informed consent. On the other hand, nation-wide initiatives based on assumed consent, have found it difficult to incorporate and justify commercial objectives. Two examples are the Icelandic deCODE[63] and the Catalan VISC+[64] initiatives. In the first case, the transfer of public health data to a unique company called deCODE Genetics Inc. never took place, and in the second case the initiative was abandoned. Reports of the European Commission about public perception of science and technology support the view that EU citizens have reservations with for-profit objectives in the context of scientific research. For example, according to the Eurobarometer, Europeans distrust researchers when they depend on private funding and consider that private financial support limits our 'ability to understand things fully'.

---

[63] Winickoff, David E., "Genome and Nation. Iceland's Health Sector Database and Its Legacy", *Innovations. Technology, Governance, Globalization,* MIT Press, Tagore LLC, 2006, pp. 80-105. doi:10.1162/itgg.2006.1.2.80

[64] Llàcer, María Rosa / Casado, María / Buisan, Lídia, "Document on Bioethics and Big Data: Exploitation and Commercialisation of User Data in Public Health Care", Publicacions i Edicions de la Universidad de Barcelona, Barcelona, Spain, 2015, pp. 51-67.

5. Conclusions

In the EU context, where policies for development, the advancement of science and technology, and socioeconomic changes have led to a knowledge-based society and economy, there are numerous initiatives to collect and use personal data to establish big data resources for health. For these types of resources, consent as previously established for traditional clinical trials or biomedical research has proven to be insufficient. Consistently, the model of consent has moved away from specific and personal informed consent towards broad or assumed consent. Generally, the first one is used in initiatives which depend on the recruitment of participants, while the second one is used in nation-wide government-based initiatives. The first one has the advantage, from the point of view of acquiring consent, of establishing direct contact with the participants, while the second one relies on general and public engagement programs.

Both of these models are a response to the objectives of big data initiatives for health, importantly the goal to support a wide range of heterogeneous research projects. This is not a negative feature of big data resources, but an intrinsic characteristic. Broad objectives are no excuse for not efficiently communicating the aims of the resource. In parallel, it is necessary to establish a two-way dialogue with the public, participants and data subjects, being transparent and honest. A decisive effort needs to be made to abandon the idea that the public needs to be 'informed' or 'educated', which assumes that the public is a passive receiver. It is a challenge to effectively incorporate the idea that the public and participants do have something important to say, and more efforts need to be done in this direction. Society is the key to the success of big data resources for health. Therefore, we should aim to create permanent communication channels that need to feed into the governance systems. Special attention must be given to the role of the private sector and to for-profit objectives that can undermine the relationship of trust with participants, data subjects and society.

The adoption of broad or assumed consent, in the case of big data resources for health, could still find a balance between the interest of the resources to support science and innovation and the protection of participants, data subjects and society. The solution is to reinforce the models of broad and assumed consent with mechanisms that made them modifiable and participative. Because of the peculiarities of health big data resources, consent must be modifiable, it should be adjustable to the will of participants

or data subjects through time. It cannot be considered a one-time opportunity that is only modifiable through an opt-out option. Instead, consent should be regarded as a valuable tool to establish the conditions of the relationship of big data resources with participants and data subjects, and to develop that relationship through time. Furthermore, consent must be participative, having to translocate some of the traditional goals of consent to representative systems. These mechanisms must ensure channels for participants to voice their will and to be included in the process of decision-making. Representative systems will acquire the responsibility to make decisions 'in the name of' participants or data subjects. In order to prevent the dilution of their autonomy, systems must truly represent their vision of life, values, expectations and interests, and protect their rights. To fulfil those objectives, big data resources depend on a permanent public engagement process to inform governance mechanisms and the processes of decision-making.

This analysis highlights the importance of the construction of a relationship based on trust and participation, where consent and governance mechanisms become key factors of success. Furthermore, it emphasises that each initiative launched in the EU is unique, because it needs to respond and adapt continuously to the particular individuals and populations involved. Finally, consent in the context of health big data resources is a key tool for paving the way to building a relationship of trust between big data resources for health and participants, data subjects and society. It is therefore absolute in its importance to ensure the success of these endeavours and strengthen the relationship of society with science and technology.

La asistencia sanitaria transfronteriza a la luz del reglamento general de protección de datos*

Cross-border health care in the light of the general data protection regulation

Daniel Jove Villares

Investigador predoctoral FPU-MECD, Universidade da Coruña (A Coruña, España)

DOI: 10.14679/1147

Sumario / Summary: 1. Introducción 2. La asistencia sanitaria transfronteriza 3. La construcción del sistema europeo de sanidad electrónica 4. El RGPD y los datos relativos a la salud 5. Consecuencias del RGPD para la asistencia sanitaria transfronteriza 5.1. Consecuencias del RGPD desde una perspectiva estatal 5.2. Las transferencias de datos entre Estados miembros 5.3. El RGPD como elemento orientador en la determinación de los datos que se pueden compartir 6. Bibliografía

Resumen / Abstract: Este trabajo analiza cómo influye la normativa de protección de datos en la asistencia sanitaria transfronteriza. Presta atención, de manera específica, a tres aspectos: los efectos en los sistemas de garantía estatales, la influencia en el modo de transferirse la información entre los Estados miembros y, finalmente, el influjo en la determinación de los datos que deben ser objeto de la historia clínica destinada a ser compartida.

This paper analyses the impact of data protection legislation on cross-border healthcare. Specifically, it focuses on three aspects: the effects on State guarantee systems influence on the transfer of information between Member States and, finally, the impact on the determination of which data should be included in the clinical record destined to be shared.

* Artículo recibido el 26 de septiembre de 2018 y aceptado para su publicación el 31 de mayo de 2019.

Palabras clave / Keywords:
RGPD / Historia clínica / Sanidad electrónica / Portabilidad / UE.
GDPR / Clinical record / e-Health / Portability / EU.

1. Introducción

El uso de las tecnologías de la información y el *big data* resulta de gran utilidad en la práctica sanitaria. No obstante, el tratamiento masivo de informaciones personales de los pacientes también supone algunos desafíos. El derecho a la protección de datos otorga al paciente unas facultades de control sobre su información personal que, adicionadas a la implementación de un sistema de garantías adecuado y a la exigencia de determinadas cautelas en la gestión de los datos, contribuirán a salvaguardar su privacidad.

En el presente trabajo se analiza cómo puede verse afectada la configuración del sistema de asistencia sanitaria transfronteriza por la adopción del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de 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)* (en adelante, RGPD).

2. La asistencia sanitaria transfronteriza

La protección de la salud es uno de los derechos fundamentales de la Unión Europea[1] (en adelante, UE). La satisfacción de este derecho hace necesario el establecimiento de un modelo de atención sanitaria capaz de asegurar la prestación de este servicio esencial a quienes vayan a circular por el territorio de la Unión.

La UE cuenta, desde los años 70, con un régimen jurídico destinado a velar por la salud de los ciudadanos cuando se encuentren en un Estado miembro (en adelante, EM) distinto del de su afiliación, estando vinculado este derecho, inicialmente, a la libre circulación de trabajadores[2]. La legislación sobre la materia fue actualizada en la primera década del siglo XXI con dos nuevos Reglamentos: el *Reglamento CE nº 883/2004, del Parlamento*

[1] Art. 35 Carta Derechos Fundamentales de la UE.

[2] *Reglamento CEE nº 1408/71 del Consejo, de 14 de junio de 1971, relativo a la aplicación de los regímenes de Seguridad Social a los trabajadores por cuenta ajena y a sus familias que se desplazan dentro de la Comunidad*.

Europeo y del Consejo, de 29 de abril de 2004, sobre coordinación de los sistemas de seguridad social (en adelante, RCSSS 2004) y por el *Reglamento 987/2009 del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 por el que se adoptan las normas de aplicación del Reglamento (CE) 883/2004, sobre la coordinación de los sistemas de seguridad social*, (en adelante, RCSSS 2009). Conforme a esta normativa, si el paciente recibe autorización en su Estado de origen[3], puede disfrutar de la misma atención que recibiría el ciudadano del país en el que se encuentre (no las de su país de origen) y bajo las mismas condiciones[4].

Sin embargo, la regulación de la asistencia sanitaria transfronteriza no se circunscribe a los mencionados Reglamentos de coordinación de los sistemas de Seguridad Social. Junto a ellos opera la *Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza*, (en adelante, DAST) [5]. Esta norma, en la que se condensa gran parte de jurisprudencia del TJUE sobre la asistencia sanitaria transfronteriza[6], viene a positivizar una concepción de la atención sanitaria entendida como un servicio y, como tal, queda amparado por la libre prestación de servicios[7]. La consecuencia fundamental para los pacientes es que, con arreglo a la DAST, pueden disfrutar, en los otros Estados miembros (EEMM), de la cartera de servicios que les correspondería en su país de filiación[8].

Existen, por consiguiente, dos regulaciones que dan sustantividad a dos modos de concebir la asistencia sanitaria. Además del modo diverso en que regulan las prestaciones a las que el paciente tiene acceso (exportación de la cartera de servicios propia al Estado de destino frente a disfrute de las atenciones en las condiciones que tendrían los nacionales de ese Estado)

---

3 Art. 20 RCSSS 2004.

4 Es importante tener en cuenta que no todos los EEMM tienen un sistema de salud idéntico, baste con indicar las diferencias en cuanto al acceso a los servicios de salud, que pueden tener carácter gratuito, requerir el pago adelantado por el paciente con reembolso posterior o ser un sistema de copago.

5 La DAST será de aplicación "sin perjuicio" de lo dispuesto en los Reglamentos, tal como establece en su art. 2.

6 Jurisprudencia que se extiende durante varios años, cuyo punto de partida se puede situar en los casos Decker y Kohll (asuntos C-120/95 y C-158/96, resueltos en 1998) y Geraets-Smits (asunto C-157/99); también han influido, especialmente en la DAST, el caso Yvonne Watts (C-374/04) o Comisión Europea contra España (C-211/08).

7 Considerando 11 DAST.

8 Aunque prestados con las condiciones del EM en que se encuentren (art. 4.1 DAST).

existen otras divergencias entre esas normas. Cantero Martínez[9] las condensa en dos, el modo de pago[10] y los sujetos habilitados para prestar los servicios sanitarios[11]. Dejando a un lado las diferencias existentes entre las normativas europeas sobre asistencia sanitaria transfronteriza[12], este trabajo se enfocará en analizar las disposiciones atinentes al tratamiento de los datos relativos a la salud en dicho ámbito.

3. La construcción del sistema europeo de sanidad electrónica

Las informaciones personales del paciente son un elemento de gran utilidad para la prestación de los servicios de salud. La asistencia sanitaria transfronteriza no es ajena a esta realidad. La transferencia de datos entre los EEMM es un instrumento idóneo (y necesario) para asegurar la continuidad en la asistencia sanitaria[13]; proporciona información precisa sobre el historial clínico del paciente, amén de ahorrar recursos materiales (v. gr. en pruebas diagnósticas) y temporales.

La DAST establece una hoja de ruta, de carácter voluntario, que tienen como finalidad la creación de una red de sanidad electrónica que facilite la cooperación y la interoperabilidad entre los EEMM[14]. Sin embargo, la materialización práctica de las previsiones normativas de la Directiva se encuentra en proceso, debido a las dificultades de implementar sistemas interoperables que permitan hacerlas efectivas[15]. Los intercambios de información, por

---

[9] Cantero Martínez, Josefa, "Los servicios autonómicos de salud ante la movilidad transfronteriza de pacientes. Su nuevo marco de obligaciones", *DS: Derecho y salud*, Núm. Extra 1, Vol. 27, 2017, p. 114.

[10] La Directiva implica que, para el paciente, el coste de la atención sanitaria debe ser el que tendría si la misma se hubiese prestado en su estado de filiación, garantizándose para el paciente el reembolso de los gastos que haya anticipado, de estar comprendida dicha atención en su cartera de servicios (art. 7.1 DAST).

[11] Conforme a la DAST también las clínicas y hospitales privados (y no solo los servicios públicos) pueden proveer los servicios sanitarios que el paciente tiene reconocidos.

[12] Sobre este particular, *vid*. Álvarez González, Elsa Marina, "La prestación de asistencia sanitaria transfronteriza. Supuestos, diferencias, similitudes y consecuencias", *Sanidad Transfronteriza y Libertad de* Circulación, Lucas Durant, Manuel / Echezarreta Ferrer, Mayte *et ál*., Ed. Tirant Lo Blanch, Valencia, España, 2018, pp. 193-241.

[13] Considerando 25

[14] Art. 14 DAST.

[15] Sobre las dificultades para establecer un sistema de e-Health a nivel europeo, *vid*. Nicolás Jiménez, Pilar / Armaza Armaza, Emilio José / Perin, Andrea, "Impact of the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare: A comparative analysis", *Revista de Derecho y Genoma Humano / Law and the Human Genome Review*, Núm. 44, 2016, pp. 59-60.

el momento, se están circunscribiendo a resúmenes de pacientes y recetas electrónicas. En este sentido, se ha optado por un proceso gradual, con fecha de inicio en 2018, en el que algunos países (8-9) han comenzado a realizar intercambios de información en los que se incluyen las historias clínicas, con el objetivo de lograr, para el año 2020, la participación de 22 EEMM[16].

Como puede constatarse, se trata de un proceso en plena evolución. En esta tesitura, resulta crucial configurar un sistema europeo de asistencia sanitaria transfronteriza capaz de hacer compatible la libertad de circulación de las informaciones relativas a la salud, y su tratamiento masivo, con el respeto del derecho a la protección de datos de los pacientes.

Las normativas sobre asistencia sanitaria transfronteriza remiten a la normativa sobre protección de datos, adoptándola como parámetro de referencia a la hora de establecer los cauces por los que el tratamiento de informaciones relacionadas con la salud de los pacientes debe transcurrir[17]. En el caso de la DAST, se remite, explícitamente, a las Directivas 95/46/CE y 2002/58/CE[18]. Por lo que respecta a los Reglamentos, estos hacen una alusión más genérica, indicando que el tratamiento ha de realizarse "con arreglo a las disposiciones comunitarias en materia de protección de las personas físicas respecto al tratamiento y libre circulación de datos de carácter personal"[19].

Desde mayo de 2018, la normativa de referencia en materia de protección de datos es el RGPD. Conocer el régimen que establece se antoja esencial para comprender los cauces por los que ha de discurrir la asistencia sanitaria transfronteriza.

---

[16] Comunicación de la Comisión relativa a la consecución de la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital, la capacitación de los ciudadanos y la creación de una sociedad más saludable de 25 de abril de 2018, p. 7. Puede consultarse *on line* en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A52018DC0233 [Última consulta: 23 de septiembre de 2018].

[17] En el caso de la DAST también se incluye el tratamiento de datos en la receta electrónica, art. 11 DAST.

[18] La Directiva 2002/58/CE, tiene por objeto la privacidad y las comunicaciones electrónicas. Esta norma será sustituida por un nuevo Reglamento que, a septiembre de 2018, se encuentra en fase de tramitación. Puede consultarse *on line* la propuesta de Reglamento en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010 [Última consulta: 23 de septiembre de 2018].

[19] Arts. 77.2 y 78 del RCSSS 2004; en el mismo sentido, art. 3.3 RCSSS 2009.

4. El RGPD y los datos relativos a la salud

Entre los elementos que caracterizan la era digital se incluye su carácter global y la consecuente necesidad de adoptar estrategias y políticas que se extiendan más allá del marco estatal. En este contexto, cobra pleno sentido que sea la UE quien establezca la norma basilar en la materia. Para lograr, así, un sistema capaz de facilitar la circulación de datos entre los EEMM y, a la vez, consolidar un marco de garantías que asegure el respeto a los derechos de los ciudadanos[20].

El RGPD ha supuesto un cambio notable respecto de la Directiva 95/46/CE. Si bien es cierto que, esta última, aportaba ciertas bases comunes, los avances acaecidos desde su promulgación, unidos a la heterogeneidad que propiciaba el amplio margen de actuación del que disponían los Estados, la convertían en un instrumento normativo poco apropiado para alcanzar unos estándares de protección adecuados.

El RGPD regula los datos relativos a la salud[21], a los que incluye entre las categorías de datos que requieren de especial protección[22]. La atribución de tal condición supone que, como norma general, su tratamiento está prohibido[23]. Sin embargo, esa disposición general puede verse excepcionada en una serie de supuestos. Entre las situaciones que habilitan el tratamiento de los datos especialmente protegidos y, en particular, los datos relativos a la salud, destacan: aquellas en las que el interesado haya prestado consentimiento; situaciones de riesgo vital (del interesado o de un tercero); cuando concurra alguno de los fines descritos en el 9.2.h), entre los que se encuentran: la medicina preventiva, el diagnóstico médico y la gestión de servicios de asistencia sanitaria (aunque los tratamientos han de realizarse por un profesional sujeto al deber de secreto[24]); también podrían ser objeto de tratamiento por razones de salud pública. En la enumeración anterior se han incluido solo algunos de los supuestos previstos en el RGPD[25], concretamente, aquellas previsiones que tienen mayor importancia para la asistencia sanitaria o, incluso, se refieren directamente a esta.

---

20 En consonancia con el considerando 6 del RGPD.

21 También define lo que ha de entenderse por dato de salud, art. 4.15 RGPD.

22 Art. 9.1 RGPD.

23 Art. 9.1 RGPD.

24 Art. 9.3 RGPD.

25 El RGPD incluye un listado detallado de las situaciones que habilitan el tratamiento de las categorías especiales de datos (art. 9.2 y 9.3). Las situaciones destacadas están previstas en el ap. 2.a), c), h), i).

5. Consecuencias del RGPD para la asistencia sanitaria transfronteriza

El RGPD menciona, de manera expresa, el tratamiento de datos en la asistencia sanitaria transfronteriza. En el considerando 35 establece que los datos utilizados en la prestación de asistencia sanitaria son datos relativos a la salud. Además, el considerando 53 incluye la "garantía de la continuidad de […] la asistencia sanitaria transfronteriza" como uno de los fines que habilitan el tratamiento de los datos relativos a la salud.

En aras de realizar una explicación más sistemática de las consecuencias del RGPD para la asistencia sanitaria transfronteriza, su estudio se abordará desde tres perspectivas. En primer lugar, se analizará cómo afecta a la gestión de la información por parte de los Estados. En segundo lugar, se tomarán en consideración los efectos que puede tener en el modo de realizar los tratamientos transfronterizos. Finalmente, se examinará de qué modo las previsiones sobre protección de datos pueden ayudar a perfilar qué informaciones han de formar parte de la documentación clínica y en qué condiciones.

5.1. Consecuencias del RGPD desde una perspectiva estatal

Los EEMM, al ser los encargados de organizar y proveer los servicios sanitarios, van a desempeñar un papel preeminente en la asistencia sanitaria transfronteriza. A la UE, por su parte, le corresponde la facultad para establecer las reglas de coordinación y actuación que faciliten la prestación de la atención sanitaria a los ciudadanos, cualquiera que sea el EM en que se encuentren.

La competencia para organizar sus sistemas sanitarios implica que cada EM puede determinar cómo va a gestionar los datos que se generen en la gestión y asistencia sanitaria. Ahora bien, el tratamiento de toda la información generada ha de estar presidido por el respeto a la protección de datos de los ciudadanos y la adecuación a las disposiciones del RGPD. No obstante, ha de advertirse que, si bien es cierto que el RGPD supone una importante armonización, no lo es menos que su articulado deja margen a los Estados para "mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud"[26].

[26] Art. 9.4 RGPD.

Los EEMM que decidan acogerse a la habilitación del art. 9.4 RGPD habrán de regularla mediante ley que, en el caso español, debería ser orgánica (al menos los artículos que regularan tales extremos). En cuanto a qué tipo de limitaciones o condiciones podrían introducir, debería tratarse de aportaciones destinadas a asegurar una mayor confidencialidad y lograr una mayor seguridad en el tratamiento. Es decir, el objetivo que debe presidir la incorporación de previsiones de ese cariz debe ser ofrecer mayores garantías al ciudadano, introduciendo obligaciones adicionales para quienes vayan a tratar ese tipo de datos. En todo caso, las limitaciones adicionales que se incorporen no pueden tener una magnitud que haga inviable llevar a efecto los fines que, con las excepciones del 9.2, se pretenden satisfacer.

5.2. Las transferencias de datos entre Estados miembros

La existencia de una norma común, así como de unos regímenes nacionales sin grandes divergencias resulta positiva para el paciente, aporta seguridad y confianza (esenciales en el ámbito sanitario) en que sus datos serán tratados con las máximas garantías, cualquiera que sea el país de la Unión en que se encuentre. Sin embargo, es en el ámbito de los tratamientos transfronterizos donde el RGPD muestra todas sus potencialidades, al eliminar las trabas normativas que pudieran impedir la libre circulación de datos entre los Estados de la UE[27]. Es tal la importancia que el legislador otorga a la circulación de datos dentro de la UE que se erige como un límite absoluto, los Estados no pueden establecer ninguna previsión que pueda, no ya impedirla, ni siquiera obstaculizarla. Esto supone que la habilitación que hace el artículo 9.4 respecto a los datos relativos a la salud (y también a los genéticos y biométricos) no podrá suponer un escollo para las transferencias de datos entre EEMM[28].

No obstante, el verdadero desafío para la consecución de ese espacio de libre circulación de información radica en la implementación de sistemas interoperables que faciliten la transferencia de datos de manera eficiente, segura, rápida y con todas las garantías.

El RGPD, con el reconocimiento del derecho a la portabilidad de los datos[29], apuesta por la creación de un marco de garantías que facilite el flujo de datos. Este derecho es de aplicación en supuestos de transmisión de datos

[27] Considerando 10 RGP.
[28] Considerando 53 RGPD.
[29] Reconocido en el art. 20 RGPD. El considerando 68 apuesta por la interoperabilidad como medio para hacer efectiva la portabilidad.

a un nuevo responsable, entre otras situaciones, cuando "el tratamiento se efectúe por medios automatizados"[30]. Se puede conjeturar que la existencia de este mecanismo, y su configuración como derecho, podrían servir de impulso para interoperabilidad. Aunque, en tanto el RGPD no establece la obligación de implementar los mecanismos para llevar a efecto la portabilidad automática, no lo es menos que puede influir en el diseño futuro de los servicios de gestión de los datos[31]. De hecho, esta será, la tendencia, en la medida en que la digitalización y automatización de los procesos de gestión y tratamiento de los datos se vaya consolidando en el sector sanitario, haciendo de la portabilidad un derecho no solo exigible sino, también, ejecutable.

5.3. El RGPD como elemento orientador en la determinación de los datos que se pueden compartir

La determinación de qué datos pueden tratarse, y en qué condiciones, es un elemento crucial en la configuración de cualquier sistema que implique operar con datos personales. El RGPD establece una serie de principios que delimitan el modo en que los datos han de ser gestionados. De los principios enunciados por el RGPD[32] aquí se analizarán dos que, por sus implicaciones, pueden tener una mayor influencia a la hora de fijar el contenido de las informaciones con las que se operará en la asistencia sanitaria transfronteriza: la pertinencia de los datos que se vayan a tratar, debiendo limitarse a aquellos necesarios para alcanzar el fin que se persigue; y la conservación de los datos, circunscrita al tiempo necesario para lograr los fines para los que fueron recabados. La problemática de estos principios radica en su aplicación en el ámbito de la asistencia sanitaria (también de la transfronteriza) debido a "la imposibilidad [de determinar], *a priori*, que […] datos de salud […] no van a ser necesarios para la atención sanitaria futura"[33].

Desde el punto de vista operativo, a la hora de regular cómo deben encauzarse las informaciones en la asistencia sanitaria transfronteriza es conveniente atender a las finalidades concretas que van a determinar cada situación. En términos generales, pueden distinguirse dos situaciones. De una parte, un escenario en el que se conoce con antelación que se va a requerir

---

30 Art. 20.1.b) RGPD.

31 El RGPD (considerando 68) señala que la portabilidad puede alentar la interoperabilidad.

32 Los principios que han de regir el tratamiento de los datos personales aparecen enunciados en el art. 5 RGPD.

33 Larios Risco, David, "La historia clínica como conjunto de datos especialmente protegidos", *El Derecho a la Protección de datos en la Historia Clínica y la Receta electrónica*, Aranzadi-Agencia Española de Protección de Datos, Navarra, España, 2009, pp. 168-169.

la prestación de servicios sanitarios en otro EM. El otro supuesto estaría representado por los casos en que la necesidad del servicio no se conoce previamente, es decir, situaciones de urgencia y sobrevenidas. Tomando en consideración los principios mencionados, los escenarios planteados van a requerir de una gestión diferente de los datos del paciente. Aunque, en ninguno de ellos parece, en principio, que "deba acudirse a un sistema de tratamiento o de historial clínico amplio, sino más bien con información relevante [y pertinente] […] que podría eliminarse una vez dejara de serlo"[34].

Cuando se tiene constancia previa del servicio sanitario que va a requerirse, la información que se comparta ha de ceñirse a la necesaria para asegurar la prestación de dicho servicio con todas las garantías. En estos casos, el período de puesta a disposición de los datos habría de ajustarse al caso concreto pudiendo extenderse, en previsión de eventuales complicaciones, durante un período adicional. Por otra parte, todas las actuaciones llevadas a cabo durante esa atención sanitaria habrían de incorporarse a la historia clínica del paciente, algo que resulta más seguro y preciso si todo el proceso se realiza mediante dispositivos electrónicos y de manera automática, sin que deba pesar sobre el paciente dicha responsabilidad[35].

En los supuestos de urgencia, por otra parte, cobra pleno sentido la existencia de unos contenidos mínimos a los que el profesional sanitario del EM en que se encuentre el paciente pueda acceder con facilidad e inmediatez. La necesidad de contar con una historia clínica electrónica que contenga una serie de informaciones básicas está prevista en la DAST[36]. En cumplimiento de esta previsión, se ha elaborado, por parte de la *eHealth Network*[37], una directriz en la que se detallan qué informaciones han de integrar la historia clínica electrónica destinada a ser compartida[38]. Esa *Guideline* está elaborada pensando, precisamente, en situaciones de urgencia, en las que

---

[34] Andreu Martínez, Mª Belén / Alarcón Sevilla, Verónica / Salcedo Hernández, José Ramón / Soro Mateo, Blanca, "Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regulación sobre protección de datos personales", *DS: Derecho y Salud*, Núm. Extra 1, Vol. 24, 2014, p. 270.

[35] Aunque la DAST también prevé la posibilidad de entregar al paciente la información de los tratamientos recibidos, art. 4.2.f).

[36] Art. 14.2.b.i) DAST.

[37] La e-Health Network es la red voluntaria de EEMM encargada de llevar a efecto las previsiones sobre sanidad electrónica Se han adherido 28 Estados y Noruega participa como observador. Más info. en: https://ec.europa.eu/health/ehealth/policy/network_es [23/09/18].

[38] *Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU*. Puede consultarse *on line* en: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf [Última consulta: 23 de septiembre de 2018].

resulta mucho más difícil determinar, *a priori*, qué informaciones se pueden necesitar. Además, hay que prever la eventualidad de que el paciente no se encuentre en condiciones de proporcionar información alguna o, sin llegar a dicho extremo, por una mera cuestión de precisión en las informaciones que pueden ser útiles al profesional y que el paciente puede no recordar, o no ser capaz de explicar en el idioma del profesional que le atiende. Los contenidos propuestos para la historia clínica básica incluyen, entre otros, información sobre alergias, vacunas, tratamientos médicos en curso, cirugías a las que se ha sometido (en los últimos 6 meses), enfermedades crónicas o informaciones relativas al consumo de tabaco o alcohol.

Para hacer efectiva la existencia de esta historia clínica básica es necesario diseñar un sistema que la deslinde de la historia clínica completa. Tal distinción es perfectamente posible desde el plano técnico, bastaría con aplicar unos estándares de acceso diferenciados, que solo permitieran acceder bajo determinadas premisas[39]. Por lo tanto, podría habilitarse un apartado que contuviera estos contenidos mínimos, al que solo se accediera en supuestos de asistencia sanitaria en otro EEMM. Debería incorporarse, además, un mecanismo que permitiera al profesional sanitario acceder a datos de la historia clínica completa no previstos en la básica. Dicho acceso quedaría reservado, exclusivamente, para situaciones en las que resultara imprescindible y previa justificación de su necesariedad.

6. Conclusiones

Conocer el historial clínico del paciente es, para los profesionales de la salud, un elemento de incuestionable valor. En tiempos pretéritos tal información estaba constreñida al profesional médico al que el paciente acudía con regularidad. Los avances tecnológicos han posibilitado que se amplíe la esfera de profesionales que pueden acceder a esa información (bajo determinadas circunstancias y con las debidas garantías).

La UE, en su proceso de integración y en aras de asegurar el derecho a la salud, también apuesta por la configuración de un sistema de asistencia sanitaria que asegure la adecuada prestación de servicios sanitarios a sus ciudadanos cualquiera que sea el Estado miembro en que se encuentren. La

[39] Sobre la implementación técnica de medidas de acceso a la Historia clínica electrónica en función de permisos, *vid*. Falcao-Reis, Filipa / Costa-Pereira, Altamiro / Correia, Manuel E., "Access and privacy rights using web security standards to increase patient empowerment", *Studies in Health Technology and Informatics*, Vol. 137, 2008, pp. 275-285.

libre circulación de las informaciones sanitarias del paciente se antoja esencial para la consecución de ese objetivo.

El RGPD ha supuesto la adopción de un marco común de garantías. Sus exigencias respecto a cómo han de tratarse los datos permiten aproximar los regímenes jurídicos de los diferentes EEMM y contribuyen a quebrar las dificultades existentes en materia de interoperabilidad.

No obstante, debe reconocerse que, en la asistencia sanitaria, existe siempre un cierto grado de incertidumbre. Ello dificulta la determinación apriorística de las informaciones que han de compartirse en supuestos de asistencia sanitaria transfronteriza. La protección de datos contribuye a solventar esta problemática al establecer ciertas reglas básicas: la adecuación a las circunstancias, la limitación del período de conservación o la minimización de los datos son principios basilares que delimitan las informaciones que se pueden compartir, y el modo de hacerlo.

En definitiva, la protección de datos y, consecuentemente, el RGPD se erigen en un instrumento eficaz, no solo para asegurar la privacidad de los pacientes sino, también, para diseñar el sistema de asistencia sanitaria transfronteriza al delimitar los modos y cauces por los que debe transcurrir el flujo de información.

7. Bibliografía

Álvarez González, Elsa Marina, "La prestación de asistencia sanitaria transfronteriza. Supuestos, diferencias, similitudes y consecuencias", *Sanidad Transfronteriza y Libertad de* Circulación, Lucas Durant, Manuel / Echezarreta Ferrer, Mayte *et ál*., Ed. Tirant Lo Blanch, Valencia, España, 2018.

Andreu Martínez, Mª Belén / Alarcón Sevilla, Verónica / Salcedo Hernández, José Ramón / Soro Mateo, Blanca, "Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regulación sobre protección de datos personales", *DS: Derecho y Salud*, Núm. Extra 1, Vol. 24, 2014.

Cantero Martínez, Josefa, "Los servicios autonómicos de salud ante la movilidad transfronteriza de pacientes. Su nuevo marco de obligaciones", *DS: Derecho y salud*, Núm. Extra 1, Vol. 27, 2017.

Falcao-Reis, Filipa / Costa-Pereira, Altamiro / Correia, Manuel E., "Access and privacy rights using web security standards to increase patient empowerment", *Studies in Health Technology and Informatics*, Vol. 137, 2008.

Larios Rico, David, "La historia clínica como conjunto de datos especialmente protegidos", *El Derecho a la Protección de datos en la Historia Clínica y la*

Receta electrónica, Aranzadi-Agencia Española de Protección de Datos, Navarra, España, 2009.

NICOLÁS JIMÉNEZ, Pilar / ARMAZA ARMAZA, Emilio José / PERIN, Andrea, "Impact of the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare: A comparative analysis", *Revista de Derecho y Genoma Humano / Law and the Human Genome Review*, Núm. 44, 2016.

Tratamiento seguro de datos como factor de integración europea: implicaciones legales en el ámbito de la salud pública en Georgia*

Safe treatment of data as a factor of European integration: legal implications in the field of public health in Georgia

Dr. Int. David Ruano Delgado

Investigador Posdoctoral del Gobierno Vasco (UPV/EHU: G.I. "Derechos Fundamentales y Unión Europea" – Université de Pau et des Pays de l´Adour: Centre de Documentation et de Recherches Européennes (Bayona, Francia)

Prof. Dr. Nikoloz Phiphia

Profesor de la Georgian Technical University: Faculty of Law and International Relations (Tiflis, Georgia)

DOI: 10.14679/1148

SUMARIO: 1. Planteamiento general. 2. El nivel de estandarización europea de la protección de datos personales en Georgia. 2.1. Cumplimiento del Convenio 108 del Consejo de Europa: la necesaria redefinición de la figura del consentimiento. 2.2. La progresiva adaptación al Derecho de la Unión Europea. 3. Aproximación al marco legal de la salud pública en Georgia. 3.1. Especial consideración de los datos relativos a la salud del paciente. 3.2. La *vis atractiva* del RGPDUE. 4. Conclusiones. 5. Bibliografía.

* Artículo recibido el 30 de enero de 2019 y aceptado para su publicación el 4 de junio de 2019.

Resumen / Abstract: La presente aportación pretende analizar el estándar europeo alcanzado por la República de Georgia en relación al derecho fundamental a la protección de datos personales en el ámbito de la salud pública, de conformidad con lo establecido en el Acuerdo de Asociación por el que rige su relación actual con la UE. De este modo, se procederá a un examen de las oportunas disposiciones legales de Derecho interno, con el ánimo de evaluar el impacto que, desde la óptica de la privacidad, ha tenido los cuatro primeros años de vigencia del Acuerdo, así como de aportar propuestas para la progresiva adaptación de aquéllas a las obligaciones introducidas por el Reglamento General de Protección de Datos.

The present contribution analyzes the European standard achieved by the Republic of Georgia in relation to the fundamental right to protection of personal data in the field of public health, in accordance with the provisions of the Association Agreement by which their relationship is governed current with the EU. In this way, we will proceed to an examination of the appropriate legal provisions of domestic law, with the aim of evaluating the impact that, from the point of view of privacy, the first four years of validity of the Agreement have had, as well as contributing with proposals for the progressive adaptation of those to the obligations introduced by the General Regulation of Data Protection.

Palabras clave / Keywords:

Protección / Datos / Integración / UE / Salud / Georgia.

Protection / Data / Integration / EU / Health / Georgia.

1. Planteamiento general

El derecho fundamental a la protección de datos de carácter personal reviste, actualmente, de un nivel de importancia impensable de predecir cuando el mismo comenzó a adquirir (por lo que se refiere al continente europeo) una cierta autonomía legislativa, doctrinal y jurisprudencial, a partir de la década de los años setenta del pasado siglo.

Dicha importancia, incrementada a la par de la evolución de las nuevas tecnologías de la informática y de la comunicación (TIC), ha venido generando una paralela regulación jurídica, tanto a escala estatal como continental, con la que se ha pretendido abordar dicha realidad, a fin de intentar aportar una solución a la problemática que entraña el cada vez más complejo *universo* de la digitalización, cual no es otra que el sometimiento de este último a los imperativos propios de un Estado democrático y, en particular, al respeto de los derechos fundamentales.

Concretamente, a nivel europeo, el primer instrumento *ratione materiae* emanaría del Consejo de Europa en 1981, el cual constituiría la referencia más próxima de la que dispondrían sus Estados parte con el ánimo de reconocer, garantizar y tutelar el derecho fundamental a la protección de datos de

carácter personal en el marco de sus respectivos ordenamientos. Incluso es más, dicho acto, que identificamos con el Convenio 108 de la mencionada organización internacional, se nos presenta como el único texto de idéntico alcance que aborda el derecho objeto de estudio, encontrándose así abierto a la firma y ratificación de cualquier país.

Así mismo, y sobre la base de los principios que aquél establece, la Unión Europea, siendo consciente que para garantizar el éxito de su objetivo integracionista (sea desde una perspectiva económica o política), no puede emprender ni desarrollar una acción desprovista de naturaleza *iusfundamental*, vendría trabajando desde el año 1990 para legislar en materia de protección de datos, con el objeto de garantizar este derecho, ya no sólo con carácter general, sino también con el propósito de hacerlo valer en el marco de las libertades económicas que conforman su Mercado interior.

Fruto de esos trabajos sería la Directiva 95/46/CE, nacida con el ánimo de armonizar el tratamiento legal de nuestro campo de estudio en los Estados miembros de la Unión, mediante su transposición, por estos últimos, a través de la aprobación de las correspondientes leyes internas. Sin embargo, la mencionada circunstancia advertida con anterioridad, referida al nivel de complejidad que, sin precedentes, viene experimentando la que denominamos *sociedad digital*, puso en evidencia las carencias de la Directiva para afrontar los nuevos desafíos que aquélla representa, necesitándose así de una reformulación y adaptación legales a los efectos de perfeccionar, y hacer más visible, la garantía del derecho en cuestión, mediante la adopción de un instrumento dotado de una mayor fuerza jurídica.

Como consecuencia de lo anterior, y tras una ardua tramitación legislativa, el derecho a la protección de datos de carácter personal se encuentra desarrollado, en el ámbito de la Unión Europea, por un Reglamento desde el 27 de abril de 2016, esto es, a través del acto legislativo más importante con el que cuenta la citada organización, el cual no sólo ha venido a suplir las necesidades observadas, sino que aporta un nuevo régimen en materia de responsabilidades y derechos, mucho más avanzado que el anterior.

Empero, el Reglamento General de Protección de Datos de la Unión Europea (RGPDUE), en vigor desde el 25 de mayo de 2016 y plenamente aplicable desde el 25 de mayo de 2018, ha ido incluso más allá que su predecesora Directiva, en lo que a su alcance territorial y efectos legales conciernen, ya que su vigencia implica, por una parte, no sólo la extensión a los Estados del Espacio Económico Europeo, sino que, en virtud de su artículo

3, el mismo presenta una vocación de universalidad que extrapolaremos, oportunamente, al campo de estudio del presente trabajo; así como, por otra, la homogeneización de legislaciones, sustituyendo en consecuencia aquellas leyes que tenían como objeto la transposición de la citada Directiva, a la que deroga expresamente.

En lo que respecta al fondo, el novedoso acto legislativo de la Unión ofrece, a su vez, un nivel de tutela tal que lo ha convertido en referente europeo de la protección de datos, hasta el punto que, como tendremos ocasión de ver, ha motivado una mejora reciente del Convenio 108 del Consejo de Europa. Ese nivel de tutela, materializado en lo que aquí nos interesa, en un refuerzo considerable de la seguridad en el tratamiento a gran escala de los datos personales sensibles y, concretamente, de aquellos de índole sanitario, vendrá a obligar, por tanto, también a los Estados que sin ser miembros de la Unión Europea, sí lo son del Consejo de Europa; reforzando, a su vez, la posición de aquellos que vienen manifestando su interés en una mayor integración con la primera de esas organizaciones y, en especial, respecto de los que lo han hecho recientemente, pues sus adaptaciones legales ostentan un mayor atractivo debido a que la aproximación legislativa debe realizarse con una mayor calidad técnica y eficacia. Máxime cuando sus intentos por avanzar en la integración lo son a largo plazo, si consideramos el punto de inflexión por el que atraviesa actualmente la Unión Europea en lo que a ese objetivo respecta.

En línea con lo anterior, la presente contribución pretende analizar la situación de uno de esos Estados, cual es la República de Georgia, lo que se justifica en el hecho de que este país del Cáucaso ha sido recientemente considerado por la Unión Europea como el referente de la Asociación Oriental, tras estar caracterizándose por un activismo pro integración en el contexto de la que se concibe como la primera etapa de un extenso camino a recorrer lentamente, con vistas a una hipotética y lejana adhesión.

A mayor abundamiento, y como se tendrá ocasión de comprobar, la pertenencia al indicado partenariado, con el que la Unión Europea viene definiendo sus relaciones de vecindad para con una serie de Estados localizados al este de sus fronteras y en el Cáucaso meridional, ofrece a estos una oportunidad para lograr no sólo el mayor grado posible de integración económica, sino además una asociación política más estrecha. Pues bien, en relación a tales objetivos, su materialización conjunta viene dada a través de la celebración de los llamados Acuerdos de Asociación, que firmados actualmente con cuatro de aquellos países (Georgia, Moldavia, Ucrania y, más

recientemente, Armenia), viene a comprometer a las partes para garantizar un nivel elevado de protección de los datos personales en los diferentes ámbitos de actividad regulados por los Acuerdos.

Considerando, por tanto, que uno de tales campos es el referente a la salud pública, y a la vista de las acciones tendentes a conseguir los objetivos marcados al respecto por el Acuerdo firmado en particular con Georgia, en el presente trabajo analizamos cómo dicho país viene implementando el estándar europeo en materia de protección de datos a los distintos sectores que engloban esa política, con el propósito de aportar una herramienta necesaria con la que evaluar el nivel de garantía del asociado derecho, tanto para los usuarios de su sistema de salud como en lo que afecta a la ejecución global de aquélla. Las conclusiones que alcancemos nos permitirán así determinar la importancia que un tratamiento de datos seguro ofrece a los efectos de alcanzar una mayor integración, dada la confianza inequívoca que puede generar un país sensibilizado con el alcance y repercusión de un derecho fundamental como es el de referencia.

2. El nivel de estandarización europea de la protección de datos personales en Georgia

2.1. Cumplimiento del Convenio 108 del Consejo de Europa: la necesaria redefinición de la figura del consentimiento

En tanto que Estado parte del Consejo de Europa desde el 27 de abril de 1999, la República de Georgia ha firmado y/o ratificado un total de 88 de los 225 convenios y protocolos que, hasta la fecha, han sido adoptados por la citada organización internacional. Aunque como es lógico, y en lo que aquí concierne, nos resulta de interés el acto por el que se vendría a obligar en relación al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, es decir, por el Convenio número 108[1], el cual comenzó a tener vigencia en el país el 1 de abril de 2006, tras firmarlo y ratificarlo los días 21 de noviembre de 2001 y 14 de diciembre de 2005, respectivamente.

[1] STE n. 108, hecho en Estrasburgo el 28 de enero de 1981. Disponible en https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108 [Última consulta: 5 de octubre de 2018].

De conformidad con lo establecido en este instrumento internacional[2], en materia de categorización de los datos personales, principios que han de regir su tratamiento, régimen de responsabilidades y sistema de derechos del titular de los datos tanto en el momento de la recopilación como de su ulterior tratamiento, así como en lo que afecta a los sistemas de seguridad y garantías adecuadas en el tratamiento, supervisión, transferencias internacionales de datos[3] y régimen sancionador, podría afirmarse que Georgia habría alcanzado el nivel de exigencia, al menos formalmente, de una manera progresiva a partir del momento en que adoptó su Ley sobre protección de datos personales el 28 de diciembre de 2011[4].

Esa progresividad se manifestaría en las continuas modificaciones sufridas por la advertida ley desde el año 2012[5], la cual además ha incorporado el

[2] Como ya se advirtiera introductoriamente, este Convenio se encuentra abierto a la firma y ratificación de cualquier país, estando incluso en vigor actualmente, además de en los cuarenta y siete Estados parte del Consejo de Europa, en Argentina (desde el 1 de junio de 2019), Cabo Verde, Marruecos (a partir del 1 de septiembre de 2019), Mauricio, México, Senegal, Túnez y Uruguay.

[3] Adviértase que la regulación contenida en materia de autoridades de control y flujos transfronterizos de datos fue completada mediante un Protocolo adicional por el que se preveía el establecimiento de autoridades de control encargadas de asegurar el respeto de las leyes y reglamentos adoptados por los Estados en aplicación del Convenio y de las disposiciones sobre tales transferencias, así como la condición de que estas últimas solo pudieran ser realizadas cuando el Estado tercero o la organización internacional de destino acreditaren un nivel de protección adecuado. El acto en cuestión se identifica con el STE n. 181, hecho en Estrasburgo el 8 de noviembre de 2001, el cual se encuentra disponible en https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181 [Última consulta: 5 de octubre de 2018].

[4] Ley de Georgia n. 5669. Disponible en https://matsne.gov.ge/en/document/view/1561437?publication=14 [Última consulta: 5 de octubre de 2018]. Habría que recordar que, al igual de lo que ocurre en el ordenamiento jurídico comparado europeo, donde el derecho fundamental a la protección de datos de carácter personal goza de un reconocimiento sustantivo propio, únicamente, en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, en Georgia encuentra respaldo constitucional en el artículo 20 de su Constitución, al abrigo del derecho a la vida privada y la libertad personal.

[5] Las modificaciones más importantes traen causa de las reformas producidas el 25 de mayo de 2012, en lo que concierne a las categorías especiales de tratamiento; el 1 de agosto de 2014, que afectaba a las definiciones, los aspectos básicos del tratamiento, la función de destrucción de información sobre datos personales obtenidos mediante investigación secreta, la inviolabilidad del inspector de protección de datos y la determinación del alcance de su autoridad, los objetivos y principios del tratamiento de datos, el propósito de la vídeo vigilancia en la vía pública y en el transporte público, la finalidad de las principales actividades de control del inspector de protección de datos, y al establecimiento de las sanciones por violación de las normas sobre transferencias de datos a otros Estados u organizaciones internacionales; y el 21 de julio de 2018, por las que se modificaban algunos términos (el inspector de protección de datos pasaba a denominarse "inspector estatal de protección de datos"), se regulaba el tratamiento de datos biométricos por parte de personas físicas o jurídicas de derecho privado, se establecía la obligación de

desarrollo reglamentario de la autoridad encargada de su cumplimiento en el país, cuyo régimen estatutario se contenía en una resolución gubernamental aprobada el 19 de julio de 2013[6]. En definitiva, una construcción legal de la que, partiendo de su versión consolidada, podemos extraer los siguientes aspectos generales de interés para nuestro estudio:

- Los datos personales de categoría especial son definidos en el artículo 2.b) de la Ley de Protección de datos personales, dentro de los cuales se incluyen expresamente los datos reveladores del estado de salud de una persona.

- Los principios que rigen el tratamiento de datos se recogen en el artículo 4, los cuales, además de identificarse con aquellos establecidos por el Convenio 108 para una gestión adecuada de los mismos (lealtad, transparencia, licitud del tratamiento, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación, integridad y confidencialidad), se desarrollan haciendo un especial énfasis en el respeto a la dignidad de la persona titular de los datos.

- El consentimiento del interesado se establece como requisito general para el tratamiento de datos en el artículo 5.

- En el artículo 6.1 se establece la regla de prohibición del tratamiento de los datos personales sensibles, salvo que, en virtud de su apartado 2, el interesado otorgue su consentimiento de manera explícita o concurra uno o varios de los supuestos específicos que se enumeran en la norma. Además, el consentimiento aludido no facultará para la difusión de los datos en cuestión, ni por la persona autorizada para su tratamiento, ni por terceros.

- Los datos personales de la persona fallecida encuentran protección en el artículo 7, estando permitido su tratamiento con fines de investigación científica, salvo que se hubiera negado expresamente en vida.

- El régimen de obligaciones y derechos de la persona autorizada para el tratamiento de datos personales, se extiende a lo largo del

notificación al Servicio de Inspección Estatal, se perfeccionaban los derechos del interesado y se determinaban las garantías apropiadas para la protección de datos.

[6] Resolución n. 180 del Gobierno de Georgia, por la que se aprueba el Estatuto regulador de las funciones del Inspector de Protección de Datos Personales, y el desempeño de su cargo. Disponible en https://personaldata.ge/manage/res/docs/unofficial%20translations/ENG%20Statute%20Unofficial%20Translation.pdf [Última consulta: 5 de octubre de 2018].

Capítulo III de la ley (arts. 15 a 20), donde se contienen la obligación de informar al interesado sobre el almacenamiento y gestión de sus datos (art. 15), el régimen al que se encuentra sometida la persona autorizada para el tratamiento de datos (art. 16), el deber de establecer medidas de seguridad adecuadas para el tratamiento (art. 17), las obligaciones conjuntas del responsable y la persona autorizada (art. 18), el contenido de los archivos o ficheros y la obligación del responsable del tratamiento de mantenerlos actualizados (art. 19), así como de informar puntualmente a la autoridad de control del país de las modificaciones sobre el contenido anterior, además de a las autoridades judiciales sobre posibles infracciones penales que hayan tenido lugar en el curso del tratamiento.

- Los derechos del titular de los datos se reconocen en el Capítulo IV de la Ley (arts. 21 a 26) y, en particular, el derecho a solicitar información sobre sus datos (art. 21), al acceso, rectificación, cancelación y oposición de los mismos (art. 22), así como el procedimiento para hacerlos valer (art. 23), las causas por las que puede limitarse su ejercicio (art. 24), además de sus derechos a negarse al tratamiento en cualquier momento (art. 25) y a recurrir ante la autoridad de control estatal, o ante instancias administrativas o judiciales, según proceda (art. 26).

- La autoridad independiente de control se regula a lo largo del Capítulo V (arts. 27 a 40), el cual entró en vigor, por las circunstancias previamente expuestas, el 1 de enero de 2019.

- El régimen de las transferencias internacionales de datos se prevé en el Capítulo VI (arts. 41 y 42).

- El sistema de infracciones y sanciones de carácter administrativo, se contiene en el Capítulo VII (arts. 43 a 55).

Incluso podría decirse que en lo que respecta a la categorización de datos, y quizá como consecuencia de la influencia que al efecto viene ejerciendo, como se verá, la normativa propia de la Unión Europea, el legislador georgiano ha ido más allá del texto en vigor del Convenio, para incluir dentro de los datos personales sensibles, ya en la versión inicial de su ley de 2011, aquellos de índole genético y biométrico[7].

[7] Adviértase que, por entonces, se desarrollaban los trabajos emprendidos por la Comisión Europea desde 2009, a fin de elaborar su Propuesta de Reglamento General de

Sin embargo, puede apreciarse cómo en un ámbito sustancial de la regulación se echa en falta, *a priori*, una delimitación más exacta del alcance del consentimiento a prestar por la persona titular de los datos, que refuerce la licitud del mismo. En este sentido, nos parece que un consentimiento general, como es el previsto en el artículo 5 de la ley, no basta para garantizar de una manera efectiva el derecho a la protección de datos, si el mismo adolece de un carácter explícito, no va acompañado además de la suficiente información sobre las consecuencias y riesgos del tratamiento, así como de una ausencia total de coacciones sobre su titular.

La circunstancia anterior se ve, además, agravada cuando se trate de un consentimiento que trascienda al específico ámbito que nos ocupa, para el que la solución aportada legalmente se antoja insuficiente, toda vez que se considera lícito, también *a priori*, un consentimiento sólo explícito para proceder al tratamiento de datos personales sensibles. Es más aún, si ello afecta a menores, el asunto entrañaría un problema mayor, puesto que la ley georgiana omite, al igual que el Convenio o la Directiva 95/46/CE, esta especificidad, tanto de manera general como particular.

Por último, y como se ha dejado intuir, el Convenio 108 del Consejo de Europa se encuentra en fase de modificación, a través de un segundo Protocolo adicional que lo vendrá a mejorar[8], con el propósito de adaptarlo a la realidad actual. Así pues, en línea con lo que se afirmara de manera introductoria, esta adaptación resulta de interés cuando se trata, en última instancia, de equiparar el nivel de tutela europeo con el acto más avanzado, y plenamente operativo, en el continente, a saber, el Reglamento General de Protección de Datos de la Unión Europea.

Tanto es así que el Protocolo en cuestión aporta al texto del Convenio una regulación mejorada del régimen de las transferencias internacionales de datos, así como un fortalecimiento del principio de cooperación entre las diferentes autoridades de control nacionales, asumiendo en consecuencia las previsiones contenidas, sobre estos ámbitos, en el acto legislativo de la Unión. Asimismo, la catalogación de los datos genéticos y biométricos, acompañado de un mayor refuerzo de las garantías para la protección de

Protección de Datos [COM(2012) 11 final, de 25 de enero de 2012], en la que la citada institución justificaba la inclusión *ex novo* de tales categorías.

8 Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal [STE n. 223, hecho en Estrasburgo el 10 de octubre de 2018]. Disponible en https://rm.coe.int/16808ac919 y su informe explicativo en https://rm.coe.int/16808ac91b [Última consulta: 11 de octubre de 2018].

los datos personales sensibles, además de unos mayores requisitos para la consideración de un consentimiento como válido, se introducen a nivel convencional, modificándose, en lo que afecta a esto último, el apartado segundo de su artículo 5 con el objeto de exigir que aquél sea otorgado de manera libre, explícita, clara e inequívoca.

No obstante, el Convenio continúa omitiendo, entre otras cuestiones, el alcance de un consentimiento prestado por menores de edad, lo que nos obliga a analizar hasta qué punto el ordenamiento georgiano es (o puede ser) más garantista de lo establecido en aquél, en base tanto a la posibilidad reconocida convencionalmente de aportar una protección más amplia como en el compromiso adquirido con la Unión en tal sentido.

2.2. La progresiva adaptación al Derecho de la Unión Europea

Considerando como incierta la vigencia temporal de la versión mejorada del Convenio del Consejo de Europa[9], y a la vista de los esfuerzos manifestados por Georgia en aras a alcanzar una mayor integración política con la Unión, procede señalar cómo en el estado actual de ese proceso, dicho país ha venido obligándose, paulatinamente, por el acervo jurídico de esta organización en diferentes ámbitos, en los que el derecho a la protección de datos personales tiene una incidencia manifiesta.

El consecuente grado de vinculación trae así causa en el Acuerdo de Asociación celebrado en 2014 entre la Unión Europea y la República de

[9] El Protocolo en cuestión se abrió a la firma el 10 de octubre de 2018 y, conforme a su artículo 37, entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses desde la fecha en la que todas las Partes de la Convención hayan manifestado su consentimiento mediante ratificación, aceptación o aprobación o, en su defecto, tras la expiración de un período de cinco años desde la fecha en que se abrió a la firma, aunque para este caso lo hará con respecto a los Estados que se hubiesen obligado por alguna de las modalidades señaladas, y siempre que el Protocolo cuente con al menos treinta y ocho Partes. De darse este último supuesto, además, y en lo que concierne a las Partes del Protocolo, todas las disposiciones del Convenio mejorado surtirán efecto inmediato tras su entrada en vigor. Asimismo, a la espera de que ello se produzca, y sin perjuicio de las disposiciones relativas a la entrada en vigor y a la adhesión de Estados no miembros del Consejo de Europa u organizaciones internacionales, una Parte del Convenio puede, en el momento de la firma del Protocolo, o en todo momento posterior, declarar que sus disposiciones le sean aplicables a título provisional. Esta declaración surtirá efecto el primer día del tercer mes que sigue a la fecha de su recepción por el Secretario General del Consejo de Europa, extendiendo los mismos efectos sólo a las Partes de la Convención que hayan realizado una declaración similar con la misma finalidad. Debe añadirse, finalmente, que en virtud del apartado 4 del citado artículo, el Protocolo adicional de 2001 (STE n. 181) quedará derogado desde la fecha de entrada en vigor del nuevo Protocolo.

Georgia[10], el cual va más allá del establecimiento de una zona de libre comercio con la que, tradicionalmente, se da inicio a un proceso de integración económica, para fijar además compromisos con el propósito de aproximar las legislaciones en distintos campos de la integración política sobre los que cooperar.

El Acuerdo de Asociación con Georgia contiene pues, en lo que nos ocupa, diferentes ámbitos de actividad que se enmarcan en la cooperación en materia de salud pública, conducentes de manera conjunta a materializar la disposición de ambas partes por mejorar el nivel de salud pública y de protección de la salud humana como condición previa del desarrollo sostenible y el crecimiento económico, tal como se prevé tanto en su preámbulo como en el artículo 355. De tales ámbitos, conforme a lo establecido en el artículo 356, destacaríamos los tres siguientes[11], dada la susceptibilidad que presentan en relación con el tratamiento masivo de datos sensibles, relacionados con el estado de salud de una persona:

- El refuerzo del sistema de salud pública de Georgia, en particular continuando con la reforma del sector de la salud, garantizando un alto nivel de calidad de la asistencia sanitaria y el desarrollo de los recursos humanos de la salud y mejorando la gobernanza y la financiación de la asistencia sanitaria;

- La vigilancia epidemiológica y control de las enfermedades transmisibles, como por ejemplo el VIH/SIDA, la hepatitis vírica y la tuber-

[10] Acuerdo de Asociación entre la Unión Europea y la Comunidad Europea de la Energía Atómica y sus Estados miembros, por una parte, y Georgia, por otra [DO L, 261 de 30 de agosto de 2014, p. 4-743]. El mismo se alcanza, como ya se introdujo, en el marco de la Asociación Oriental de la UE, a través de la cual se concibe la dinámica actual de la política de vecindad de la Unión con seis países de la Europa oriental y del Cáucaso meridional (Armenia, Azerbaiyán, Bielorrusia, Georgia, Moldavia y Ucrania), pudiéndose diferenciar dos visiones contrapuestas: por un lado, la de aquellos Estados (caso de Azerbaiyán y Bielorrusia) que prefieren obviar los fines integradores que tal alianza podría favorecer, limitándose a la firma de acuerdos puntuales de tipo comercial o económico; y la de los cuatro restantes, por otro, que han manifestado su interés por reforzar sus vínculos con la Unión, llegando incluso a solicitar (caso de Georgia, Moldavia y Ucrania) el reconocimiento expreso de su integración a la misma, mediante la firma de los Acuerdos que comentamos. En tal sentido, léase Rodríguez Prieto, V., *La actuación normativa de la Unión Europea en la Asociación Oriental. Los casos de Georgia y Moldavia (2009-2018)* – Marcial Pons, Madrid, España, 2018.

[11] Completan este capítulo las materias relativas a la calidad y seguridad de las sustancias de origen humano, la información y conocimientos sobre la salud, y la aplicación efectiva de los acuerdos internacionales en materia de salud suscritos por las Partes, en particular las normas sanitarias internacionales y el Convenio Marco para el Control del Tabaco.

culosis[12], así como de la resistencia a los antimicrobianos[13], y mejora de la preparación frente a las emergencias y las amenazas para la salud pública;

- La prevención y control de las enfermedades no transmisibles, principalmente intercambiando información, y mejores prácticas, fomentando hábitos de vida saludables y el ejercicio físico y haciendo un seguimiento de los principales factores determinantes de la salud, como la nutrición, la adicción al alcohol, las drogas y el tabaco.

Empero, el desarrollo de las mismas, siguiendo con lo que venimos argumentando, no podrá hacerse sin las debidas garantías del derecho fundamental concernido. Es aquí, por tanto, donde encontramos la base normativa que justificaría los avances de Georgia en lo referente a la protección de datos personales, y amparados en la normativa específica de la Unión, pues en virtud del artículo 14 del Acuerdo, las Partes convienen en cooperar a fin de garantizar un nivel elevado de protección de los datos personales de conformidad con los instrumentos y normas de la UE, el Consejo de Europa e internacionales, referidos expresamente en el Anexo I del mismo Acuerdo[14], y

---

[12] Al respecto, véase, la Resolución del Parlamento Europeo de 5 de julio de 2017, *sobre la respuesta de la Unión al VIH/SIDA, la tuberculosis y la hepatitis C* [DO C, 334 de 19 de septiembre de 2018, p. 106-111] donde la institución europea, en su preocupación por hacer frente al recrudecimiento de tales epidemias en los países de la Europa oriental y del Asia Central, aboga por emprender, aprovechando las sinergias de la Asociación Oriental, un marco de acción global e integrado desde la Unión, mediante el desarrollo de las oportunas medidas de cooperación transfronteriza, apoyo económico e intercambio de información.

[13] Sobre el particular, consúltese el documento de la Comisión Europea denominado *Plan de acción contra la amenaza creciente de las resistencias bacterianas* [COM(2011) 748 final], donde se recogen 12 acciones que deben poner en práctica los Estados miembros de la Unión Europea, así como 7 ámbitos en los que resulta imprescindible tomar medidas en tal sentido. Igualmente, el Parlamento Europeo, dictaría su Resolución de 11 de diciembre de 2012, *sobre el desafío microbiano: la creciente amenaza de la resistencia a los antimicrobianos* [DO C, 434 de 23 de diciembre de 2015, p. 49-58]; mientras que el Consejo adoptaría, más recientemente, sus Conclusiones *sobre los próximos pasos para combatir la resistencia a los antimicrobianos en el marco del planteamiento "Una sola salud"* [DO C, 269 de 23 de julio de 2016, p. 26-30], y *sobre los próximos pasos para hacer de la UE una región modelo en materia de buenas prácticas en la lucha contra la resistencia a los antimicrobianos* [DO C, 214 de 25 de junio de 2019, p. 1-7].

[14] Considerando que el citado Anexo se enmarca en el contexto del desarrollo de un Espacio de Libertad, Seguridad y Justicia, no podemos obviar la aplicación de instrumentos específicos cuando en ella trasciendan cuestiones relativas al tratamiento de datos personales. En este sentido, se establece que cada una de las Partes del Acuerdo tendrá en cuenta la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, *relativa a la protección de datos personales tratados en el marco de la cooperación policial*

ya citados en el presente estudio, a saber, la Directiva 95/46/CE y el Convenio 108 del Consejo de Europa, junto a su Protocolo de 2001.

En definitiva, profundizar en este asunto nos obliga, ineludiblemente, a tener que aproximarnos a la legislación sectorial del país con el objeto de advertir sus necesidades de cara a lograr una consolidación del estándar fijado por el Acuerdo de Asociación, así como su adecuación progresiva, y obligada, al marcado por las nuevas disposiciones contenidas en el Reglamento General de Protección de Datos de la UE[15] y en el Protocolo de mejora del Convenio 108 del Consejo de Europa. No obstante, en este momento debemos defender que será el primero de los dos instrumentos citados el que ha de servir como referencia prioritaria, por las siguientes razones:

- Porque al haber derogado la Directiva, sería incoherente mantener un alcance del derecho a la protección de datos en base a la misma, cuando la otra parte viene ya rigiéndose por un nivel de protección más elevado, lo que podría provocar disfuncionalidades en la aplicación del Acuerdo de Asociación;

- En relación con lo precedente, y tal como se ha avanzado, la vigencia del Protocolo de 2018 se antoja incierta en el tiempo, de manera que esperar a la misma podría interrumpir el proceso de integración europea. Una circunstancia que se evitaría si estimamos que Georgia, en base al Acuerdo de Asociación, puede considerarse obligada por un instrumento, incluso, más garantista, como es el Reglamento; y

---

y judicial en materia penal, y la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, *dirigida a regular la utilización de datos de carácter personal en el sector de la policía*. No obstante, siguiendo la lógica planteada en las presentes líneas, ha de observarse que el nivel de tutela en lo que respecta, al menos, a la Unión Europea en este ámbito, ha variado desde el momento en que la citada Decisión Marco fue derogada por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos* [DO L, 119 de 4 de mayo de 2016, p. 89-131], cuyo plazo de transposición expiró el pasado 6 de mayo de 2018.

[15] 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)* [DO L, 119 de 4 de mayo de 2016, pp. 1-88].

- Porque, en refuerzo de lo anterior, este último está investido, como se verá en el siguiente apartado, de una vocación universalista, permitiendo con ello que sus principales novedades vinculen a terceros Estados.

3. Aproximación al marco legal de la salud pública en Georgia

3.1. Especial consideración de los datos relativos a la salud del paciente

Con carácter previo a abordar el impacto que el nuevo instrumento de la Unión Europea tendría, en materia de protección de datos, para el campo de la salud pública georgiana, y en consonancia con las apreciaciones esgrimidas en las líneas que preceden, resulta menester estudiar las disposiciones que guardan relación con los objetivos extraídos del contenido del artículo 356 del Acuerdo de Asociación, pues ello nos aportará una idea certera sobre la magnitud de las repercusiones que, en su derecho positivo, se derivarán de aquél.

En particular, cabría citar los siguientes textos normativos, ordenados cronológicamente:

- Ley n. 1139 de 10 de diciembre de 1997, de Atención Sanitaria.
- Ley n. 160 de 23 de febrero de 2000, sobre Trasplantes de órganos humanos.
- Ley n. 283 de 5 de mayo de 2000, sobre los Derechos del Paciente.
- Ley n. 904 de 8 de junio de 2001, sobre Práctica Médica.
- Ley n. 1172 de 7 de diciembre de 2001, sobre Examen Médico y Social.
- Ley n. 3451 de 14 de julio de 2006, de Atención Psiquiátrica.
- Ley n. 5069 de 27 de junio de 2007, de Salud Pública.
- Ley n. 2042 de 17 de noviembre de 2009, sobre la prevención y control de infección por VIH/SIDA.

- Ley n. 6245 de 22 de mayo de 2012, sobre estupefacientes, sustancias psicotrópicas y precursores, y asistencia narcológica.

- Ley n. 4629 de 11 de diciembre de 2015, sobre el control de la Tuberculosis.

De todos ellos, lo primero que habría que subrayar es que las respectivas versiones consolidadas tienen como última modificación conjunta el 5 de julio de 2018, guardando correspondencia con un desarrollo coherente de las líneas de actuación marcadas en el artículo 356 del Acuerdo de Asociación, lo que viene motivado, a su vez, por la aprobación de un Decreto gubernamental por el que se aprueba una agenda de reformas para el período 2014-2020, con el ánimo de potenciar la asistencia sanitaria universal y un control de calidad en la protección de los derechos del paciente[16].

Resulta por ello destacable cómo, en lo que concierne al tratamiento de datos del paciente en su interrelación con el sistema sanitario del país, se produce un avance garantista más allá de lo previsto, con carácter general, en la ley sobre protección de datos. Una circunstancia que trae causa, sobre todo, en el ejercicio sensibilizador que, en relación al alcance del derecho fundamental que analizamos, se encuentra realizando la autoridad de control georgiana en diferentes materias y, más exactamente, en el ámbito de la salud, donde tiene publicada una recomendación[17] de 2016 en la que se reconoce indubitadamente que la información sobre el estado de salud de una persona contiene, en ciertos casos, aspectos íntimos de su vida personal, así como de su condición mental y física, pudiendo servir su tratamiento ilegal como base para lesionar, estigmatizar o discriminar a su titular. Es esto último lo que, precisamente, motiva al órgano indicado a afirmar la importancia de que una persona albergue una sensación de expectativa legítima sobre la protección de la confidencialidad respecto de la información

[16] Decreto n. 724 del Gobierno de Georgia, de 26 de diciembre de 2014. Disponible en https://www.matsne.gov.ge/en/document/view/2657250?publication=0 [Última consulta: 5 de octubre de 2018]. No obstante, y a la luz del paquete legislativo ya existente sobre la materia en el país, sería interesante impulsar una futura codificación o refundición con la que supera una eventual disparidad en el tratamiento de la cuestión, tal como ha venido proponiéndose por ejemplo en España. En este sentido, léase por todos, Barreda, I., "Protección de datos de salud (III), vértices legales de la confidencialidad", *Actualidad del Derecho Sanitario*, Núm. 212, 2014, p. 102-111.

[17] Disponible en https://personaldata.ge/manage/res/images/news-image/2016/recomendations/Health%20Data%20Reccomendation.pdf [Última consulta: 5 de octubre de 2018].

que le concierne, ya que en el caso de una confianza inadecuada, podría abstenerse de proporcionar información importante, pudiendo así dificultar el establecimiento de un correcto diagnóstico o la aplicación del tratamiento médico adecuado, lo que a juicio de la oficina georgiana de protección de datos, tendría un impacto negativo no sólo para la salud de la persona, sino incluso para la eficiencia del mismo sistema de salud.

En este sentido, la Ley sobre los Derechos del Paciente[18] ha venido a perfeccionar la regulación que observábamos anteriormente sobre el alcance del consentimiento, en sintonía con la especial protección que merecen los datos objeto de tratamiento en este contexto. De este modo, su artículo 28 establece que procederá el tratamiento de datos relativos al estado de salud del paciente, por el personal médico competente, cuando:

a) los mismos se obtengan a través de un consentimiento informado de su titular;

b) la no difusión de la información contenida en los datos ponga en peligro la vida y/o salud de terceros;

c) la información sobre el paciente sea utilizada con fines de investigación científica o médica, y siempre que resulte imposible la identificación del paciente; o

d) por otras causas expresamente contempladas en la legislación de Georgia.

No obstante, la protección de los datos de esta naturaleza no es sólo de interés para la persona del paciente, sino que la Ley de Georgia sobre Práctica Médica[19], en su artículo 48, estipula que todo profesional médico estará obligado, en el ejercicio independiente de su profesión, a respetar la confidencialidad de la información sobre el estado de salud y la vida privada de un paciente en el curso de la implementación de la praxis médica o tras su finalización, tanto durante la vida como después de la muerte del paciente. Asimismo, se prevé que el indicado profesional tendrá derecho a tratar dicha información confidencial para los casos determinados expresamente por la legislación del país, siendo de especial atractivo para nuestro trabajo, aquellos

[18] Disponible en: https://www.matsne.gov.ge/en/document/view/16978 [Última consulta: 5 de octubre de 2018].

[19] Disponible en: https://www.matsne.gov.ge/en/document/view/15334?publication=19 [Última consulta: 5 de octubre de 2018].

vinculados a razones de interés público en el ámbito de la salud pública o con fines de investigación científica.

Lo anterior cobra aún más importancia al comprobar que se aporta, incluso, un tratamiento específico del consentimiento prestado por los menores de edad en tal escenario, el cual ha venido siendo objeto de mejora por las dos últimas modificaciones de la Ley sobre los Derechos del Paciente. Por consiguiente, de sus artículos 39 a 43 se deduce que el otorgado por los menores de 16 años no será considerado válido, salvo que se trate de una información especialmente sensible sobre su salud, que pueda menoscabar su dignidad[20]. Asimismo, se exige en todos los casos a que se refieren los mencionados preceptos, que el consentimiento sea informado, tanto cuando tenga como objeto la prestación de un tratamiento médico como en aquellos supuestos en los que legalmente proceda la información correspondiente a sus padres o representante legal.

Por último, en lo que al tratamiento de tales datos respecta, puede apreciarse cómo el mismo se ajusta a los principios informadores analizados anteriormente, de tal forma que se procesarán de manera justa y legal, debiendo el personal sanitario tener un objetivo legítimo y claramente definido al efecto, no estando permitido el tratamiento de datos con fines incompatibles a aquél. Esta adecuación resulta extensible también al régimen de derechos del titular de los datos, pues se reconoce al paciente el derecho a recibir toda la información relacionada, a conocer con exactitud qué tipo de datos sobre su persona se procesan y/o almacenan en una institución médica, con el objeto bien de recopilar información a efectos estadísticos, elaborar su historial médico o analizar los resultados de pruebas médicas. El paciente tiene, igualmente, derecho a elegir la modalidad de ceder sus datos y a que la información sobre el estado de su salud le sea proporcionada con claridad.

[20] Se trata de una restricción del derecho que asiste, con carácter general, a los padres o representantes legales, de obtener una completa información sobre el estado de salud del menor, justificada en el hecho de preservar la dignidad de este último. En particular, las excepciones alcanzan los supuestos de los menores emancipados y de aquellos en los que, siendo el paciente un menor de edad entre catorce y dieciocho años que, pudiendo evaluar su estado de salud adecuadamente en opinión de un profesional médico, hubiere solicitado a un médico el tratamiento para el cuidado de enfermedades de transmisión sexual o contra la adicción a las drogas, o el asesoramiento sobre métodos anticonceptivos no quirúrgicos o para la interrupción artificial del embarazo. En tales casos, cuando el paciente esté en contra de la entrega de información a su padre o representante legal, el personal de atención médica vendrá obligado a observar el secreto de la información, debiéndose siempre realizar la consulta médica con el menor separadamente.

3.2. La vis atractiva del RGPDUE

El grado de garantía legal de la protección de datos en el ámbito sanitario puede considerarse como el mejor ejemplo de la superación, por parte de Georgia, del estándar de tutela ofrecido al respecto por el Consejo de Europa en la materia, corroborando así un mayor acercamiento al que se deriva de la normativa de la Unión. En este sentido, podría deducirse su equiparación al que se desprendía de la derogada Directiva 95/46/CE, a partir de la cual se configuraron unos determinados derechos[21] para la persona del paciente que han sido extendidos, por la Unión Europea, incluso al ámbito de la asistencia sanitaria transfronteriza[22].

Circunstancia, la anterior, que refuerza las consideraciones vertidas previamente en defensa del Reglamento General de Protección de Datos de la UE como instrumento de referencia actual a los efectos de establecer un nivel de protección más avanzado y perfeccionado. Máxime cuando las consecuentes transferencias, así como el tratamiento de su contenido, se producen de manera digitalizada, implicando un riesgo elevado e inherente tanto para la confidencialidad de los datos como para la dignidad de su titular[23].

---

[21] Desde la doctrina y la jurisprudencia se vendría a identificar y reconocer el derecho de las personas a acceder a los datos personales relativos a su salud, que figuran, por ejemplo, en el historial médico del paciente, que contiene informaciones tales como el diagnóstico, los resultados de exámenes, las evaluaciones de los médicos a cargo del paciente y todo tratamiento recibido o intervención practicada. Sobre el consecuente estándar de protección, véase Ferraud-Ciandet, N., "Sécurité et confidentialité des données de santé dans l´Union européenne. Le cadre légal applicable aux dossiers médicaux électroniques nationaux", *Journal de Droit européen*, 2009, pp. 12-14.

[22] Lo que tuvo lugar a través de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, *relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza* [DO L, 88 de 4 de abril de 2011, pp. 45-65]. Instrumento que ha sido valorado recientemente por la Comisión Europea, a los efectos de analizar su impacto, mediante su Informe de 21 de septiembre de 2018 [COM(2018) 651 final], el cual se encuentra disponible en: https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-651-F1-ES-MAIN-PART-1.PDF [Última consulta: 11 de octubre de 2018].

[23] Al respecto, véase la Resolución del Parlamento Europeo, de 14 de marzo de 2017, *sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* [DO C, 263 de 25 de julio de 2018, p. 82-89], o el reciente estudio del Parlamento Europeo *Digitalisation and Big Data: Implications for the health sector*, el cual recoge las principales conclusiones de un *Workshop* organizado en Bruselas el pasado 19 de junio de 2018. Disponible en: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282018%29619030 [Última consulta: 5 de octubre de 2018].

Siendo consciente de ello, y partiendo de la solución que el nuevo acto legislativo de la Unión aporta a los efectos de satisfacer las exigencias derivadas de tal realidad[24], la autoridad de control de protección de datos de Georgia ha elaborado una recomendación específica sobre el tratamiento de los datos personales en la asistencia sanitaria[25], donde fija detalladamente en qué términos debe llevarse a cabo el tratamiento de datos por el personal sanitario, desde que se produce la identificación del paciente hasta que se almacenan en el sistema electrónico y se proceda a su destrucción, pasando por el establecimiento de un régimen sobre su empleo para la elaboración de toda documentación médica (incluyendo posibles estudios biológicos), así como a los efectos de regular su divulgación y el tratamiento de datos de una persona fallecida[26].

En particular, hemos de recalcar cómo al referirse a las medidas tendentes a garantizar adecuadamente la confidencialidad del paciente, establece que las mismas han de tener un alto nivel de seguridad tecnológica a los efectos de acceso a los datos, entendiendo que debe considerarse el empleo de técnicas de *seudonimización* por las que se decanta el Reglamento. Asimismo, se prevé un régimen específico para el tratamiento con fines de investigación científica o médica, obligando a que el consentimiento otorgado por el paciente a tales efectos tenga carácter implícito, debiendo aquél ser informado sobre el almacenamiento de los datos, su accesibilidad y posible transferencia.

Incluso es más, pues en ese mismo documento se aboga por garantizar un sistema de derechos del interesado en plena sintonía con lo establecido en el artículo 7 del Reglamento de la Unión, haciendo prevalecer un consentimiento para considerar lícito el tratamiento que, aunque deba ser expresado en los mismos términos que los advertidos en sede de la versión mejorada

[24] Resulta así de interés la guía elaborada por la Oficina del Inspector Estatal de Protección de Datos titulada *¿Qué debemos saber sobre el Reglamento de Protección de Datos de la Unión Europea?*, disponible en: https://personaldata.ge/manage/res/docs/GDPR.pdf [Última consulta: 11 de octubre de 2018].

[25] Disponible en: https://personaldata.ge/manage/res/docs/%E1%83%AF%E1%83%90%E1%83%9C%E1%83%93%E1%83%90%E1%83%AA%E1%83%95%E1%83%98%E1%83%A1%20%E1%83%A0%E1%83%94%E1%83%99%E1%83%9D%E1%83%9B%E1%83%94%E1%83%9C%E1%83%93%E1%83%90%E1%83%AA%E1%83%98%E1%83%90.pdf [Última consulta: 5 de octubre de 2018].

[26] Resulta procedente, llegados a este punto, recordar el hecho de que el Reglamento General de Protección de Datos de la UE, conforme a su Considerando n. 27, resulta inaplicable a la protección de datos de las personas fallecidas, quedando reservada a los Estados miembros la competencia para establecer normas relativas al tratamiento de los datos personales de estas.

del Convenio 108, no se concibe con carácter absoluto, previéndose así la excepción relativa al caso de que el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos, o a su necesidad por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar mayores niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios. Aunque eso sí, se establece que en este último supuesto, el tratamiento deberá ir acompañado del establecimiento de medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional[27].

En última instancia, debemos acometer un análisis sobre el ámbito de aplicación territorial del Reglamento, a los efectos de reforzar la extensión de su fuerza vinculante hacia Georgia. De este modo, como se ha venido afirmando, dicho instrumento nace con una vocación de universalidad que, en interés del campo que nos ocupa, se traduce en una delimitación más exacta que aporta del citado alcance con respecto a lo que hacía la Directiva 95/46/CE, así como en el sometimiento a sus disposiciones tanto por el sector público como privado.

En consecuencia, el artículo 3 del Reglamento toma también en consideración la localización extra-europea del establecimiento del responsable del tratamiento, a fin de garantizar que una persona física no quede excluida de la protección a la que tiene derecho en virtud del mismo. De este modo, hace extensivas las garantías en él contenidas a toda persona que se encuentre en territorio de la Unión, con independencia de su nacionalidad, obligando a los establecimientos que radiquen fuera de aquél y, más exactamente, en un lugar donde el derecho de un Estado miembro se aplique en virtud del Derecho Internacional Público[28], lo que en el presente caso vendría motivado tanto por la naturaleza jurídica como por el alcance de los instrumentos examinados propios del Consejo de Europa.

---

[27] Así nos lo recuerdan De Terwangne, C. / Rosier, K. / Losdyck, B., "Le règlement européen relatif à la protection des données à caractère personnel: quelles nouveautés? ", *Journal de Droit européen*, 2017, p. 308.

[28] De interés resulta el estudio realizado sobre este extremo por Pailler, L., "L´applicabilité spatiale du Règlement général sur la protection des données (RGPD) – Commentaire de l´article 3", *Journal du Droit International*, Núm. 3, 2018, pp. 823-849.

4. Conclusiones

El derecho fundamental a la protección de datos personales, especialmente en el ámbito de la salud, es uno de los asuntos prioritarios e importantes en Georgia. En tanto que autoridad independiente de control, la Oficina del Inspector de Protección de Datos Personales de Georgia y, en general, el Gobierno de Georgia, vienen caracterizándose por desarrollar una actividad inequívocamente orientada, por un lado, a respetar la privacidad de la persona y la protección de sus datos personales y, por otro, a facilitar el funcionamiento y la eficacia del sistema de salud del país, siendo considerables los avances producidos en el campo de la atención médica y sanitaria.

Considerando así ese escenario de concienciación, debe concluirse que alcanzar un nivel de tutela de dicho derecho por el indicado Estado, en base al ofrecido por el Reglamento General de Protección de Datos de la UE, no ha de considerarse como un ambicioso reto o desafío de alcance legislativo, sino más bien como el siguiente paso natural a la luz del estado actual de las disposiciones internas que resultan de aplicación, en materia de salud pública, en pro de alcanzar los objetivos marcados por el Acuerdo de Asociación con la Unión.

No obstante, la vigencia de este nuevo instrumento plantea una serie de cuestiones que, en la práctica, se conciben como las principales materias sobre las que, el legislador georgiano, podría abordar una oportuna reforma legal a corto plazo. En particular, debe apreciarse la necesidad de definir, expresamente, el alcance del consentimiento del titular de los datos, con carácter general, conforme a las exigencias establecidas tanto en el artículo 7 del Reglamento como en la versión mejorada del Convenio 108 del Consejo de Europa, así como en lo que respecta al prestado por los menores de edad. Destaca, en este último extremo, que el régimen ofrecido por la legislación sectorial de Georgia se adapta a los criterios aportados por el Reglamento en su artículo 8.

En otras palabras, lo anterior iría en aras de lograr una mayor seguridad jurídica, sin perjuicio de que tal consentimiento venga interpretándose conforme a la línea jurisprudencial marcada por el Tribunal Europeo de Derechos Humanos, a cuya jurisdicción queda sometida la República de Georgia en su condición de Estado parte del Consejo de Europa.

Finalmente, en lo que respecta al perfeccionamiento de las medidas de seguridad en el tratamiento de estos particulares datos, así como de las garantías adecuadas para salvaguardar la confidencialidad de sus titulares, se deberá tener como referencia los nuevos estándares fijados por el Regla-

mento, más aún si tal información es procesada mediante la utilización de sistemas electrónicos, debiendo la normativa georgiana avanzar en el sentido de la concreción de aquellas medidas y garantías, especialmente cuando el tratamiento se materialice en una transferencia de datos a otros países u organizaciones internacionales, puesto que la regulación actual, aunque ajustada a los parámetros establecidos en el primer protocolo adicional al Convenio 108 del Consejo de Europa y en la Directiva 95/46/CE de la Unión Europea, no sólo ha devenido obsoleta según se desprende de las descritas reformas llevadas a cabo en sede de ambas organizaciones, sino que también podría verse superada por un escenario en el que la probabilidad de que una persona nacional de Georgia quede dentro del ámbito de aplicación del Reglamento, se vea incrementada por el Acuerdo de Liberalización de visados en vigor desde el 28 de marzo de 2017, así como por la participación del país en diferentes programas de movilidad auspiciados por la Unión.

5. Bibliografía

Barreda, Iñigo, "Protección de datos de salud (III), vértices legales de la confidencialidad", *Actualidad del Derecho Sanitario*, Núm. 212, 2014.

Chaltiel, Florence, "La protection des données personnelles. À propos de l´entrée en vigueur du règlement général de protection des données", *Les Petites affiches*, Núm. 111, 2018.

De Terwangne, Cécile / Rosier, Karen / Losdyck, Bénédicte, "Le règlement européen relatif à la protection des données à caractère personnel: quelles nouveautés?", *Journal de Droit européen*, 2017.

Degrave, Elise, "La protection des données à caractère personnel enfin réformée", *Journal de Droit européen*, 2016.

Ferraud-Ciandet, Nathalie, "Sécurité et confidentialité des données de santé dans l´Union européenne. Le cadre légal applicable aux dossiers médicaux électroniques nationaux", *Journal de Droit européen*, 2009.

Herveg, Jean / Van Gyseghem, Jean-marc, "La protection des données à caractère personnel en droit européen", *Journal européen des droits de l´homme*, Núm. 1, 2017.

Pailler, Ludovic, "L´applicabilité spatiale du Règlement général sur la protection des données (RGPD) – Commentaire de l´article 3", *Journal du Droit International*, Núm. 3, 2018.

Rodríguez Prieto, Victoria, *La actuación normativa de la Unión Europea en la Asociación Oriental. Los casos de Georgia y Moldavia (2009-2018)* – Marcial Pons, Madrid, España, 2018.

Vayr, Jonathan / Blum, Patrick, "Le RGPD, révolution ou évolution?", *Les Petites affiches*, Núm. 126, 2018.

Una aproximación al *big data* y al *blockchain* sanitario y su implicación en la protección de datos personales*

An approach to big data and health blockchain and their involvement in the protection of personal data

Lorena Pérez Campillo

Investigadora de la Universidad del País Vasco UPV/EHU, Doctoranda UC3M

Abogada ICAM especializada en Derecho Tecnológico (Madrid, España)

DOI: 10.14679/1149

Sumario / Summary: 1. Introducción. El dataísmo. 2. Una aproximación al *Big Data* en *e-Health*. 3. *Blockchain* Sanitario. 4. Conclusiones.

Resumen / Abstract: A mayor flujo de información, mayor será el impacto en el derecho fundamental de protección de datos personales máxime en el sector de la salud digital. El binomio de *big data y blockchain* propicia un "ecosistema" donde actores y participantes (por ejemplo, hospitales, médicos, investigadores, universidades, aseguradoras, farmaceúticas, etc..) interactúan e intercambian información con seguridad y legalidad.

The greater the flow of information, the greater the impact on the fundamental right to protection of personal data, especially in the digital health sector. The binomial of big data and blockchain propitiates an "ecosystem" where actors and participants

* Artículo recibido el 28 de septiembre de 2018 y aceptado para su publicación el 3 de junio de 2019.

Para la realización de este trabajo se ha contado con el apoyo del Proyecto de Investigación EUCANCan:

A federated network of aligned and interoperable infrastructures for the homogeneous analysis, management and sharing of genomic oncology data for Personalized Medicine. Funded by the European Union's Horizon 2020 research and innovation programme and the Canadian Institutes of Health Research. Grant Agreement number: 825835.

(for example, hospitals, doctors, researchers, universities, insurance companies, pharmaceuticals, etc.) interact and exchange information with security and legality.

Palabras clave / Keywords:

Big data / *Blockchain* sanitario / Protección de datos personales / *e-Health*.

Big data / Health blockchain / Personal data protection / e-Health.

1. Introducción

En el futuro, los hospitales estarán en Internet, la información genética invadirá el *cloud (*convirtiéndose en el "cloud genético"), las investigaciones más exitosas se realizarán a través de analítica de los macrodatos y, las personas podrán vender sus datos obtenidos a través de sus *wearables* a organizaciones farmacéuticas por medio de plataformas de *blockchain*. En 2025, el mercado de *blockchain* sanitario superará los 1,600 millones de dólares[1]. Con tecnologías disruptivas presentes y venideras, los científicos esperan que en el 2049 no sea necesario acudir al médico, bastando un simple "selfie" con un *smartphone* para tener un diagnóstico clínico. En concreto, el binomio de las tecnologías *big data y blockchain* originará un papel facilitador y simplificador para analizar y tratar datos confiables de salud en el marco del ecosistema de actores y participantes. Ambas, en conjunto, posibilitarán transparencia, confianza, seguridad, exactitud, verificación y simplicidad.

Ahora bien, los modelos comerciales, también en la industria de la salud digital están explotando nuevas formas de recolección masiva, transmisión instantánea, combinación y reutilización de información personal para fines imprevistos y con dudosas y opacas políticas de privacidad. Esto pone en una situación comprometida al derecho fundamental de protección de datos, inclusive con la llegada del nuevo Reglamento General de Protección de Datos (RGPD), el cual no puede, ni debería, ser un obstáculo para la innovación y el desarrollo de estas tecnologías en esta industria. Ya el SEPD[2] llamó la atención a los expertos en privacidad en el informe anual del 2016 para examinaran los conceptos de la tecnología *blockchain* y la forma mejor de implementar el RGPD. Por su parte, el Parlamento Europeo, en el mes de julio de 2019, responde a las solicitudes de *stakeholders* y autoridades nacionales de

---

1 Estudio. *La cadena de bloques en el mercado de la salud superará los USD 1,600 millones de dólares en 2025.* Disponible en: https://es.cointelegraph.com/news/study-blockchain-in-healthcare-market-to-surpass-16-billion-by-2025 [Última consulta: 10 de septiembre de 2019]

2 European Data Protection Supervisor (EDPS), *Annual Report,* 2016. Disponible en: https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf [Última consulta: 10 de septiembre de 2019]

control de protección de datos, redactando el documento "Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?"[3]

2. Una aproximación al *big data* en *e-health*

Las empresas tecnológicas comienzan a crear sus propias herramientas de *big data*, como es el caso de *Siemens* (*Teamplay)*, –donde ya cuentan con 153 Instituciones conectadas a la red con más de 2.500 equipos activos compartiendo datos y convirtiéndolos en información y 300.000 estudios realizados– o *Apple* (*HealthKit)* que posibilita transmitir registros médicos electrónicos –con datos como el peso, calorías y ritmo cardíaco– a la Universidad de Standford para su investigación.

Por su parte, por ejemplo, la Universidad de Sidney ha realizado un estudio del análisis de la forma facial[4] para detectar marcadores de salud fisiológica en más de 270 individuos de diferentes etnias, y así conocer el índice de masa corporal y la presión arterial. En la genómica, también ha llegado el *big data* analítico, por ejemplo, los investigadores del CNIO desarrollan *PanDrugs*, una herramienta de prescripción de medicamentos que tiene en cuenta los datos genómicos del paciente.

2.1. Retos y posibles soluciones en materia de protección de datos.

Ahora bien, también es el momento de estudiar los retos específicos que surgen en el ámbito de los proyectos de *big data y eHealth*, como, por ejemplo:

i. *La discriminación o* "dictadura de los datos"

La generación de perfiles de consumidores o *profiling* es sin duda uno de los usos principales del *Big Data*, y puede entrañar riesgos por posibles tratamientos basados en predicciones si se utilizan de forma discriminatoria

[3] European Parliament, *Blockchain and the Data General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* Disponible en: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf [Última consulta: 10 de septiembre de 2019].

[4] "¿Cómo diagnosticar enfermedades a través de la forma del rostro?", *Salud Digital.* Disponible en: https://www.consalud.es/saludigital/94/como-diagnosticar-enfermedades-a-traves-de-la-forma-del-rostro_45763_102.html [Última consulta: 10 de septiembre de 2019].

excluyendo a sectores minoritarios en base a los resultados analizados, lo que se viene denominando "la dictadura de los datos" (ISMS AEPD, 2017). En este sentido, podemos decir que uno de los mayores problemas que tiene el *Big Data* es lo que denominan como "*obscurity by design"* de los algoritmos (*Hartzog y Stuzman*, 2013, 386)[5]. La regulación actual tiene por objeto último evitar la *discriminación* y garantizar la libertad dando primacía a la dignidad del paciente o consumidor y al cumplimiento normativo.

ii. *La compatibilidad con el principio de finalidad, consentimiento y el continuo cambio*

No siempre se conoce, desde el inicio, el alcance del proyecto *big data* y sus finalidades. En este sentido, el responsable del tratamiento deberá hacer referencia a que los datos personales no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. El Comité Internacional de Bioética (IBC) de la Unesco propone un nuevo modelo de consentimientos más adecuados a la naturaleza de la tecnología: el consentimiento amplio, de exclusión y dinámico. Este último requerirá de una actualización sobre el uso de datos de forma continua para que el individuo pueda optar por usos específicos. Investigador y paciente estarían conectados y podría funcionar como una empresa prácticamente (Consejo Nuffield, 2015)[6] donde se podría instaurar cierto equilibrio de poder.

iii. *La falta de autonomía individual y de transparencia*

El IBC en su informe[7] sobre *Big Data* y *e-Health* trata la cuestión de la f*alta de autonomía individual,* estableciendo que incluye entre otras cosas, la competencia del individuo interesado para acceder, comprender, evaluar, aplicar información relevante y decidir con los medios apropiados y de la existencia de diferentes opciones, la voluntariedad (Mertz *et ál.*, 2016)[8]. Por

[5] Hartzog, Woodrow / Stutzman, Frederic D., "Obscurity by Design*", Washington Law Review,* Vol. 88, 2013. Disponible en: https://ssrn.com/abstract=2284583 [Última consulta: 10 de septiembre de 2019].

[6] Nuffield Council on Bioethics, *La recopilación, vinculación y uso de datos en biomedicina investigación y cuidado de la salud: cuestiones éticas*. Disponible en: http://nuffield-bioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf [Última consulta: 10 de septiembre de 2019].

[7] Comité Internacional de Bioética, *Informe del IBC sobre big data y salud.* Recuperado de http://unesdoc.unesco.org/images/0024/002487/248724e.pdf [Última consulta: 10 de septiembre de 2019].

[8] Mertz, M. / Jannes, M. / Schlomann, A. / Manderscheid, E. / Rietz, C. / Woopen, C., *Digitale Selbstbestimmung,* Centro de Ética, Derechos, Economía y Social de Colonia Ciencias de la Salud, 2016. DOI 10.8716 / ceres / 00001

otro lado, el Dictamen WP203[9] señala que para que exista transparencia, los individuos deberán tener acceso a sus perfiles y a sus fuentes y a la lógica de la toma de decisiones, es decir, a la lógica de los algoritmos. Lo más sensible no es tanto el contenido sino las inferencias que se pueden producir.

iv. *La anonimización no irreversible*

En el contexto de la Sociedad de la Información en la que vivimos, la información (personal) es un recurso fundamental para todos los participantes. Ahora bien, el desarrollo inminente de la tecnología puede afectar e impactar a los derechos fundamentales de las personas físicas si no se toman las cautelas y medidas adecuadas para protegerlos. Sin medidas como la anonimización irreversible, nuestra información podría ser combinada con diferentes patrones y estaría totalmente desprotegida. Por ello, este uno de los mayores riesgos a los que nos podemos enfrentar y, más difícil de encontrar soluciones técnicas.

Tal y como señala la guía de la AEPD sobre "Orientaciones y garantías en los procedimientos de anonimización de datos personales"[10];

> "la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de estos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales".

No es para nada desdeñable el hecho de que la LOPDGDD (apartado p, art. 72.1) señale como infracción muy grave a la anonimización reversible o anonimización no irreversible[11].

En cualquier caso, hay que tener muy presente el objetivo de la anonimización tal y como se señala en la guía;

---

[9] GT29. *Dictamen 03/2013 sobre la limitación de la finalidad*. (WP 203). Disponible en: https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp203_en.pdf [Última consulta: 10 de septiembre de 2019].

[10] AEPD, *Orientaciones y garantías en los procedimientos de anonimización de datos personales.* Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf Pto. 8

[11] El legislador señala, en concreto, en dicho artículo, como infracción muy grave a "la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados".

"En el proceso de anonimización se deberá producir la ruptura de la cadena de identificación de las personas. Esta cadena se compone de microdatos o datos de identificación directa y de datos de identificación indirecta. Los microdatos permiten la identificación directa de las personas y los datos de identificación indirecta son datos cruzados de la misma o de diferentes fuentes que pueden permitir la reidentificación de las personas, como la información de otras bases de datos de este u otro responsable, de las redes sociales, buscadores, blogs, etc".

En este sentido, sería bastante útil para el lector, asimilar cuestiones relacionadas con el propio proceso de anonimización, como por ejemplo; determinar la finalidad de los datos anonimizados como el uso científico o los plazos de conservación, establecer variables confidenciales necesarias para el tratamiento de los datos, eliminación de datos identificativos como son los nombres, fechas de nacimiento, email, teléfono, DNI, dirección IP, fotografía, etc.; o la utilización de rangos para "enmascarar" a las personas o contar con una política de claves[12] para ocultar la identificación.

Sin embargo, y a pesar del esfuerzo por intentar conseguir una posible anonimización irreversible, no se albergan grandes esperanzas sobre esta técnica, y en dicho documento así lo deja esclarecer:

"No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen" [13].

---

[12] Pero si hablamos del proceso de anonimización, deberíamos hablar de la utilización de claves y algunas técnicas señaladas por la AEPD como; (i) algoritmos de hash; (ii) algoritmos de cifrado; (iii) sello de tiempo; (iv) capas de anonimización; (v) perturbación de datos; (vi) reducción de datos. Quisiera destacar la importancia, por un lado, de la técnica del sello del tiempo que garantiza la fecha y la hora en la que la anonimización han sido realizada y por otro lado, de las capas de anonimización, donde el legítimo destinatario asegura (con una segunda capa) con sus propios recursos de anonimización. Esta doble capa se pude utilizar atendiendo a la clasificación de las variables, de la organización interna o de garantías específicas de la política de anonimización.

[13] En este sentido, la AEPD aconseja entre otras medidas, técnicas que requieran un *coste lo suficientemente alto que la* "reidentificación" resulte ser inviable o inasumible en términos de "esfuerzo-beneficio". Por tanto, como podemos esperar, será necesario, por un lado, *valorar los riesgos* de esa *reidentificación* y por el otro, tomar y elegir *medidas organizativas* (como la definición de un equipo de trabajo, la formación del personal, las

El avance de la tecnología y los grandes volúmenes de información disponibles hacen difícil garantizar el "anonimato absoluto"[14]. Piénsese en el desarrollo de la computación cuántica y la vulnerabilidad de la seguridad[15] de la información que ésta puede generar sino se avanza, por ejemplo, en la encriptación cuántica.

A continuación, intentaremos aproximarnos lo más posible a algunas soluciones como:

i. *Ética de datos y responsabilidad proactiva del responsable*

Partimos de la idea de que la ética y la *accountability*[16] son fundamentales para cualquier proyecto vinculado a *Big data*. El SEPD señala que la responsabilidad de dar solución al reto de la Era de la digitalización podría reposar en un ecosistema interdependiente de desarrolladores, empresas y reguladores a miras del interés del individuo. Se refiere a las personas físicas como personas empoderadas –o "*prosumidores"*– las cuales producen y consumen contenido y servicios. A éstas se les tendría que dotar de más control sobre sus datos por medio, por ejemplo, de uso de almacenes o bóvedas de datos.

ii. *Privacidad desde el diseño y EIPD*

En concreto, el responsable del tratamiento aplicará medidas técnicas y organizativas (art. 25 RGPD) apropiadas, como la seudonimización, la minimización de datos, y garantías necesarias. Dentro de las medidas de responsabilidad activa exigidas por el RGPD también se encuentra la Evaluación

---

medidas de confidencialidad, el uso de posibles estándares, la utilización de códigos de buenas prácticas, etc.) para conseguir una anonimización irreversible.

[14] *Vid.* Martínez Martínez, Ricard, "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", *Revista Valenciana d'Estudis Autonòmics*, Núm. 62, 2017, pp. 257-259. Disponible en: http://www.transparencia.gva.es/documents/19318353/165265446/RVEA+62+v2-1+Completo.pdf

[15] Ordenadores cuánticos: el fin de la seguridad. *Kaspersky.* Disponible en: https://www.kaspersky.es/blog/ordenadores-cuanticos-el-fin-de-la-seguridad/1632/ [Última consulta: 10 de septiembre de 2019].

[16] El GT29 ya consideraba que las medidas comunes de responsabilidad, pueden ser, entre otras, establecer procedimientos internos previos a los tratamientos; establecer políticas escritas (o más bien acciones que no se queden en papel) donde se contemplen los criterios de calidad, los principios de seguridad, de acceso, notificaciones; el nombramiento del DPO, formaciones a los trabajadores; establecer mecanismos de quejas interno–, establecer mecanismos de notificación internos de violaciones de seguridad, auditorías internas y externas…etc.

de Impacto (art.35) siendo obligatorio para procesamientos de alto riesgo, en los que se incluyen los datos de salud.

iii. *Gobierno de datos y anonimización*

Los sistemas de control, monitorización y anonimización junto a políticas preventivas, proactivas y mitigadoras de riesgos internas que cubran lo que no está cubierto en los marcos legales serán las herramientas para utilizar por el delegado de protección de datos (DPO) o el comité multidisciplinar que trabaje para este fin. El problema no es tanto si se puede eliminar el riesgo y producir la reidentificación por completo sino si se puede mitigar el riesgo hasta que sea totalmente improbable.

Por otro lado, como establece la AEPD e ISMS (2017, 30), "aunque los procesos de anonimización y disociación son clave para respetar la privacidad en los análisis de *Big Data*, no hay que desdeñar *otras medidas técnicas* aplicables al desarrollo de cualquier sistema, aunque con particularidades propias para su aplicación a *Big Data*[17].Y a su vez, estas técnicas podrían estar contenidas en algunas implementaciones en función de la fase de *big data* en la que el proyecto se encuentre (Ver Tabla I).

3. *Blockchain* sanitario

Si hemos hablado de *big data* en el apartado anterior, a continuación, abordaremos *blockchain* y de esta manera, conseguiremos entender porque puede ser tan interesante la combinación de ambos.

Dentro de poco, los pacientes dispondrán de aplicaciones móviles donde los pacientes de hospitales públicos y privados podrán acceder mediante *blockchain* (junto con *IoT*, por ejemplo), y permitirán compartir la información de sus historiales clínicos electrónicos con aseguradoras médicas para solicitar presupuestos de pólizas o con profesionales de salud u hospitales para ayudar en el diagnóstico o con farmacias o *startups* tecnológicas de *e-Health* para colaborar en investigaciones biomédicas. Un estudio[18] reveló

[17] *Vid.* Cloud Security Aliance (CSA). *Expanded Top Ten Big Data Security and Privacy Challenges.* Disponible en: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf [Última consulta: 10 de septiembre de 2019].

[18] Blockchain Technology Market. Global Opportunity Analysis and Industry Forecast 2018 – 2025. Disponible en: https://www.meticulousresearch.com/product/blockchain-market/ [Última consulta: 10 de septiembre de 2019].

increíbles predicciones para la industria del *blockchain*, un crecimiento anual compuesto del 74,1%, equivalente a 28 millones de dólares para el 2025. En concreto, el *blockchain* en el mercado sanitario se espera que se valore en $ 5,61 mil millones para ese año.

Ahora bien, profundicemos en el concepto. Un *blockchain* es esencialmente una infraestructura digital que agrupa registros de transacciones en bloques con sello de tiempo (de ahí el nombre). Estos son registrados por todos los participantes (nodos) de una red dada. Cada nuevo bloque hace referencia al anterior con hashes criptográficos, creando un registro inmutable de todas las transacciones desde el primer bloque hasta el último.

Las transacciones están certificadas para ser verdaderas, no porque una autoridad confiable (por ejemplo, un banco central, el gobierno, Facebook, etc.) valide la contabilidad centralmente, pero porque el ledger se distribuye en tiempo real a todos los participantes de la red. Un participante de la red no puede falsificar el registro, porque un algoritmo de consenso reconcilia la información a través de los nodos, detectando cualquier discrepancia. Esto significa que cada participante, es decir, paciente, sabe en todo momento lo que ha sucedido. *Blockchain* permitirá que un paciente o consumidor de fármacos pueda identificarse en la Red sin tener que otorgar sus datos personales y, a su vez donar o *monetizar* sus propios datos genómicos. Por lo que todo ello supone una auténtica revolución en los derechos individuales (y fundamentales), comunicaciones y negocios.

Por ejemplo, en la actualidad, en Dubai existen unas cabinas inteligentes *(Bodyo)* en los centros comerciales que utiliza IoT, IA y *Blockchain,* donde se emplean sistemas de recompensa a través de *smart contracts* para aquellas personas que muestran un buen "comportamiento de salud".

En definitiva, ¿por qué esta tecnología se ha podido penetrar en la Industria del Cuidado de la Salud? Por diferentes motivos como los siguientes:

i. *El envejecimiento poblacional en los países desarrollados y las limitaciones presupuestarias*. Las nuevas iniciativas del sector se pueden centrar, según la empresa Capital Cell[19], en tres campos como son la introducción de datos médicos personalizados en *Blockchain*, la compartición de datos médicos con fines de investigación y desarrollo

[19] "Blockchain, pieza clave para nuestra salud", *Salud Digital*. Disponible en: https://www.consalud.es/saludigital/109/blockchain-pieza-clave-para-nuestra-salud_49823_102.html [Última consulta: 10 de septiembre de 2019].

de nuevos fármacos, y la trazabilidad en la producción y el consumo de medicamentos.

ii. *Debido a la desconexión entre la sanidad pública y la privada*. ¿Disponer de todos los datos médicos de lideres internacionales?

Un ejemplo de *blockchain* sanitario es la alianza entre la ***Administración de Alimentos y Medicamentos de Estados Unidos*** (**FDA**) e ***IBM Watson Health*** para explorar el uso de *Blockchain* en el uso compartido de información médica. El convenio incluye el intercambio de datos de pacientes procedente varias fuentes, incluyendo registros médicos electrónicos, ensayos clínicos, datos genómicos y datos de salud procedentes de dispositivos móviles, *wearables e Internet of Things*. Otro ejemplo, es la alianza entre *Alibaba Health Information Technology* y el Gobierno Chino que pretende almacenar los datos del sistema de salud a través de *Blockchain*. La empresa tecnológica pretende conectar la infraestructura médica con el sistema de tratamiento médico. Por su parte, la *Estonian eHealth Foundation* está asegurando los registros médicos de más de un millón de pacientes. El sistema es totalmente transparente y cualquier paciente puede iniciar sesión y ver exactamente quién ha estado viendo sus registros e incluso puede restringir el acceso a grupos de usuarios. De igual forma el *gobierno de Dubái* también ha lanzado un proyecto para establecer una plataforma *blockchain* para hacer más eficiente a la administración, crear industria y liderazgo internacional. Respecto a las empresas tecnológicas, IBM *Watson Health* y la FDA se han aliado para investigar conjuntamente sobre el intercambio seguro, eficiente y escalable de datos de salud usando *blockchain*. Aunque no hay una regulación concreta para este protocolo, se ha puesto en marcha de la iniciativa de normalizar a nivel internacional (ISO/TC 307) las tecnologías de registro electrónico distribuido y en particular, el protocolo *blockchain.*

La mejor manera de entender el sistema es diseñando un ejemplo de ecosistema con participantes o actores que intervienen (Ver Tabla II).

Este es un sistema de *blockchain* cerrado y permisionado, diferente, por tanto, del blockchain público de *bitcoins*. Es necesario tenerlo en cuenta.

Pero ¿qué papel tienen los participantes como sujetos jurídicos frente a la normativa europea en protección de datos? (*Prima facie*, un posible esquema relacionando posiciones jurídicas podría ser el de la Tabla III)

Detengámonos en esto, y veamos, aunque sea de forma pormenorizada, el rol que podrían adoptar. *Responsable* (art. 4.7. RGPD y 24 RGPD) es la persona física o jurídica que determina los fines y los medios para procesar los datos personales. Por lo que cualquiera que acceda a los datos almacenados en una cadena de bloques y haga tratamiento de datos (art. 4.2. RGPD) *según sus propios fines* se convierte en responsable de tratamiento. Además, se puede dar que el tratamiento se lleve a cabo por una asociación de participantes en una *blockchain* donde todos se considerarían corresponsables (Art. 25 RGPD). En caso de ser así, en ella se deberán *definir las obligaciones y responsabilidades de cada uno* respecto del cumplimiento del RGPD.

Y, por otro lado, *¿cómo se considerarían a los nodos (validadadores) y mineros?* Sólo si tienen un papel más activo se les consideraría "responsables del tratamiento". Esto ocurrirá cuando decidan sus propios fines, el hardware y el software.

Por otro lado, recordemos que el *encargado*, es cualquier persona física o jurídica que trata los datos personales en nombre del responsable (art. 4.8 RGPD) o también se define[20] como la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste. *Cuando los nodos ejecutan las instrucciones* del responsable *y verifican* que la transacción cumple con los criterios técnicos, por ejemplo, un formato y un cierto tamaño máximo, y que el participante tiene capacidad para realizar su transacción. En este caso, se podrían tratar de los mineros, y se les podría considerar como "full nodes"[21]. Por tanto "sólo algunos tipos de nodos descargan toda la cadena de bloques y contribuyen a validar y apoyar el libro mayor compartido, y el nivel de participación de en el tratamiento de los datos varía en función del algoritmo de consenso y en función de el nivel de apertura de la configuración de la cadena de bloques" (Giannopoulou, 2018, 9)[22].

---

[20] Autoridad Catalana de Protección de Datos (APDCAT). *El encargado de tratamiento en el Reglamento General de Protección de Datos (RGPD).* Disponible en: http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf [Última consulta: 10 de septiembre de 2019].

[21] Hay que tener en cuenta las diferencias ya que los mineros procesan bloques y los nodos completos verifican si las transacciones que han sido empaquetadas en el bloque por los mineros son todas válidas. Algunos pueden ejecutar un nodo completo sin ejecutar el software de minería. Para más info sobre el debate existente ver foro en: https://bitcoin.stackexchange.com/questions/59220/what-is-the-difference-between-a-miner-and-a-full-node

[22] Giannopolou, A. / Ferrari, V., Distributed Data Protection And Liability On Blockchains. *INTERNET SCIENCE. 5th International Conference, INSCI 2018*. St. Petersburg, Rusia,

Además, también se encuentran los proveedores de *blockchain*, como, por ejemplo, es *HSBlox*, quienes dan soluciones tecnológicas a pacientes (pensemos en asociaciones de pacientes o consumidores de servicios *eHealth*) o a proveedores de salud (hospitales) o a pagadores (empresas farmacéuticas).

En el sistema expuesto se podrán realizar las siguientes acciones:

- Acceso por parte del *e-paciente/e-usuario* a sus datos de salud desde cualquier sitio y dispositivo conectado a Internet, a través de una aplicación móvil o web.

- Acceso por parte de *otros actores (hospitales/centro médicos, profesionales sanitarios)* a los datos de las personas físicas interesadas, siempre que este acceso haya sido permitido explícitamente y de antemano bien por el paciente o bien por el centro médico productor del dato. Estos permisos pueden concederse o revocarse en cualquier momento y se almacenan en la blockchain.

- Acceso a datos anonimizados de forma agregada para uso en investigación por parte de los diferentes *universidades o centros investigadores* pueden participar si son incluidos en la blockchain privada para consultar datos. Los propios pacientes pueden otorgar y revocar el uso para investigación de sus datos, así como ver para qué fueron utilizados. Si bien no todos los proyectos de *blockchain* implican el procesamiento de datos personales, en la práctica, muchos usos de este protocolo requieren la manipulación de estos datos, tanto en términos de contenido como de información de los participantes.

Pero ¿cómo se producen los tratamientos de datos personales? Se puede producir por la intervención de los usuarios, nodos validadores y mineros cuando envían, verifican y almacenan o registran las transacciones. Tengamos en cuenta dos tipos puntos de vista respecto al tratamiento en *blockchain*:

i. En primer lugar, pensemos en *el tratamiento de datos como servicio (per se),* por ejemplo, el sistema de dinero electrónico entre igual e igual. Los medios serán el software y el hardware que los nodos y mineros utilizan para este fin. Estos últimos son quienes deciden sus propios fines, el hardware y el software a utilizar. Dicho esto, enten-

Octubre 24-26, Proceedings, Vol. 2. Workshops, 2018, p. 9. Disponible en: https://pure.uva.nl/ws/files/31868271/SSRN_id3316954.pdf

deríamos que los *nodos validadores y mineros* serán los *responsables del tratamiento.*

ii. En segundo lugar, pensemos en el tratamiento de datos que se produce en una *transacción individual y específica,* del que nos referiremos a partir de ahora. Los medios en este caso son elegidos por la propia plataforma *blockchain*. Los usuarios proporcionan los datos personales en el sistema al enviar sus transacciones. El papel de los nodos y los mineros es facilitar el acceso a la base de datos y el papel de los usuarios determinar qué datos se almacenan. Dicho lo cual, entenderíamos que los *responsables del tratamiento* serían los *usuarios* (o participantes).[23]

Hemos hablado de participantes y de tratamiento, pero hablemos de datos personales. En este sentido, es de destacar el considerando 26 RGPD, donde el legislador señala que los datos personales *pseudonimizados* se deben considerar información sobre una persona física identificable. Además, apunta que para determinar si una persona física es identificable, debe tenerse en cuenta *todos los medios* que *razonablemente* pueda utilizar el responsable del tratamiento o cualquier otra persona *para identificar al individuo*. Por ejemplo, "las claves y direcciones públicas desechables de *Bitcoin* pueden calificarse como datos personales" (Finck, 2018, 12)[24].

Según la CNIL, un *blockchain* puede contener dos categorías de datos personales:

i. *Identificación de participantes* donde *cada participante tiene una clave pública, que garantiza la identificación del emisor y el destinatario de una transacción.* Según la CNIL, los participantes, podrían ser considerados como responsables de tratamiento en la medida que decidan sobre los fines y los medios de procesamiento.

[23] Este ejemplo de caso de uso comienza con un médico que agrega un nuevo registro siguiendo los siguientes pasos: (i) La información del registro se almacena en el sistema de base de datos existente del proveedor; (ii) Se publica una referencia hash a los datos (con los permisos de visualización apropiados) en la cadena de bloques a través de nuestro cliente *Ethereum* y la biblioteca de API de *backend*; (iii) El paciente puede recuperar y descargar estos datos de la base de datos del proveedor, luego de que el controlador de acceso a la base de datos verifique el *blockchain* para confirmar sus derechos de acceso y propiedad.

[24] Fink, M., "Blockchains y Protección de datos en la Unión Europea", *Der Juristiche Verlag Lexxion,* Núm. 1, Vol. 4, 2018, pp. 17-35. Disponible en: https://edpl.lexxion.eu/article/edpl/2018/1/6/display/html [Última consulta: 10 de septiembre de 2019].

ii. *Datos adicionales escritos "en" una transacción* (por ejemplo, HCE, registros de médicos personales de wearables de pacientes). Si estos datos se refieren a personas físicas, posiblemente distintas de los participantes, directa o indirectamente identificables, se tratarán de datos personales.

Las características de este sistema *blockchain* serían:

i. *Acceso integral e intercambio de datos.* El paciente interactúa con multitud de proveedores de atención médica (médicos, dentistas, enfermeros etc.), y en cada momento, dejan datos dispersos en lugares diferentes dificultando el acceso y rastreo de los datos fragmentados. El sistema de *blockchain* podría facilitar una *"one-stop-shop"* a través de *smart contracts*.

ii. *Descentralización y cifrado.* Los datos se almacenan localmente en bases de datos separados de los pacientes y proveedores. Cuando el médico agrega un nuevo registro se almacena, se publica una referencia hash en la cadena de bloques, el paciente podrá recuperar y descargar estos datos una vez que el controlador verifique el *blockchain* para confirmar sus derechos de acceso y propiedad.

iii. *Equilibrio de poder y autonomía del paciente.* Sería posible una economía de datos entre consumidores y productores de datos que, en el campo de investigación médica, en la industria farmacéutica, en las AAPP, en compañías de seguro y otros interesados. Los pacientes podrían cambiar de médico, revisar su historial descargándolo en la última cadena de bloques de la red.

Analicemos a continuación las implicaciones del *blockchain* en materia de protección de datos y el RGPD.

i. En primer lugar, el *consentimiento* (cf. 4.11, 6.1.a y 7 RGPD) *expreso* que es obligatorio en la nueva regulación no entraría en conflicto, sino todo lo contrario, podría resultar un elemento clave para el cumplimiento puesto que el usuario verifica y valida los datos antes de que se agreguen a la cadena de bloques. El problema de la asunción errónea de legitimación en entornos de ensayos clínicos ha hecho que investigadores[25] estudien el potencial de *blockchain* como

[25] Benchouf, M. / Ravaud, P., "Blockchain technology for improving clinical research quality", *BMC Trialsjournal*, 2017, Disponible en: https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z [Última consulta: 10 de septiembre de 2019].

solución. Y es que la FDA estadounidense ha informado que casi en el 10% de los ensayos no se obtuvo un consentimiento informado por escrito o los formularios de los individuos estaban sin aprobar o los documentos otorgaban un consentimiento no válido.

ii. En segundo lugar, respecto al ejercicio de los derechos de los titulares de datos como el de *derecho de acceso y portabilidad* (art. 15 y 20 RGPD) según la CNIL, se podrían ejercer de manera efectiva.

iii. En tercer lugar, respecto a la *privacidad desde el diseño* (cf. Art. 25 RGPD), podemos decir que la propia infraestructura de la tecnología, o más bien, del protocolo, es la que obliga la utilización de seudónimos (donde no pueden atribuirse a un interesado sin utilizar información adicional) y algoritmos desde el momento inicial del proyecto. Pero no sólo eso, sino que la propia CNIL recomienda a los actores que implantan proyectos tecnológicos planteen el protocolo *blockchain* en lugar de otras alternativas.

iv. En cuarto lugar, al igual que cuando un dispositivo se extravía con información cifrada y sin poder acceder a su contenido, habrá que notificar a la autoridad de control y a los interesado puesto que no queda afectada la *confidencialidad* pero si la *disponibilidad* (cf.art.1.f, 33 y 24 RGPD).

Ahora bien, hablemos de los retos respecto a la compatibilidad con el RGPD.

i. En primer lugar, *blockchain* es un protocolo no una tecnología, por lo que intentar determinar quién es el *responsable de tratamiento* (cf.4.7 y 24 RGPD) puede ser contradictorio. Se trata de un un sistema descentralizado por naturaleza, y no encaja con el modelo de dicotomía de responsable/encargado de tratamiento. No existe un sujeto que se responsabilice del mismo.

ii. En segundo lugar, tampoco resulta posible aplicar el *derecho de supresión* (art. 17 RGPD) o "*derecho al olvido",* rectificación (art. 16 RGPD) en un sistema donde los datos ingresados en la cadena de bloques son imborrables e inrectificables toda vez que la transacción se valida.

iii. En tercer, y en línea de lo anterior, tampoco sería posible casar la obligación de la limitación del periodo de conservación (art. 5.1. e RGPD) puesto que *blockchain* se caracteriza por la *inmutabilidad de los datos*.

iv. Y en cuarto lugar, los actores de *blockchain* públicos necesitarán estar atentos ante las *subcontrataciones* y a las normas de trasferencias internacionales. Piénsese por ejemplo, en los desarrolladores de *smart contract* donde organizaciones farmacéuticas moneticen los datos extraídos a través de aplicaciones de medicamentos con *wearables*.

Si pensamos en aproximaciones a posibles soluciones a los puntos críticos del RGPD podemos apuntar a las siguientes conclusiones:

i. *Respecto a los posibles riesgos generales en protección de datos*. Resultará de aplicación (y de gran utilidad) la realización de la evaluación de impacto o EIPD (art. 35 RGPD) debiendo analizar la novedad del *blockchain* en función del nivel de conocimiento de la organización. Corresponderá a los actores implantar el tipo de *blockchain* que ponga en menor riesgo a los derechos y libertades de las personas físicas analizando la necesidad y la proporcionalidad.

ii. *Respecto a la anonimización y la dificultad de que sea irreversible.* Se podría apostar por soluciones tecnológicas que hagan posible alejar todo riesgo de reidentificación. Desde las autoridades europeas se están estudiando.

iii. *Respecto a la inmutabilidad y derecho al olvido*. La inmutabilidad en *blockchain* se debe principalmente a la criptografía, al árbol de *Merkle* y al algoritmo de consenso, pero no dotan a esa de una rigidez absoluta. La CNIL, por ej., está evaluando soluciones tecnológicas que sin que obtengan resultados idénticos a lo que establece el RGPD permitan acercarse *especialmente cortando la accesibilidad de los datos de acuerdo con el formato elegido (compromiso criptográfico, cifrado, huella dactilar resultante de una función hash ...).*

iv. *Respecto a la responsabilidad.* Si bien nadie es responsable de esta tecnología, si se pudiera identificar a alguien como causante de una agravio, se le podría exigir a éste responsabilidad civil o derecho de daños, y responsabilidad penal por posibles conductas de manipulación fraudulenta de la cadena de bloques según el art. 248.2 CP

en relación con estafas mediante instrumentos informáticos, o en el art. 264 en relación con la alteración de documentos electrónicos ajenos (González-Meneses, 2017, 106)[26]".

v. Respecto a la libertad contractual. Ibáñez (2018,160)[27] señala que *"el legislador debe permitir que los operadores jurídicos en el momento de programar un smart contract (SC), puedan diseñar clausulas parametrizables en los contratos que tienen lugar entre las partes para su ejecución en una blockchain dando cabida a la autonomía de la voluntad de forma que estas puedan flexibilizar las condiciones del negocio mediante opciones guiadas, bajo el principio de consentimiento informado, introduciendo avisos de mutación si es preciso en el propio SC"*[28].

4. Conclusiones

El binomio de *big data y blockchain* origina un papel facilitador y simplificador para analizar y tratar datos confiables de la e-salud en el marco del ecosistema de actores y participantes pero plantean desafíos a la regulación existente. *Blockchain*, de hecho, será más efectivo siempre en combinación con otras tecnologías, como por ejemplo, internet de las cosas o *machine learning*. El desarrollo tecnológico posibilitará, no a largo plazo, en el campo de la salud, el avance hacia una sociedad desarrollada y saludable. No obstante, cuanto mayor sea el flujo de información que intervenga en las tecnologías, mayor será el riesgo e impacto en los derechos de las personas. Como bien es sabido, la maquina legisladora no siempre llega a tiempo de la irrupción tecnológica por lo que, en ocasiones podemos encontrarnos con vacíos, lagunas o bloqueos legales a la hora de aplicar la normativa. Es entendible que los legisladores no alcancen a entender aspectos escrupulosamente técnicos tal y como se requeriría habida cuenta el escenario presente. Y es la propia naturaleza de cada una de las tecnologías la que en ocasiones hace complicado acercarse al "absoluto cumplimiento normativo".

---

[26] González-Meneses, Manuel, *Entender Blockchain: Una introducción a la Tecnología de Registro Distribuido,* Ed. Thomsons Reuters Aranzadi, España, 2017, p. 106.

[27] Ibañez Jiménez, J., Wenceslao, *Blockchain: Primeras cuestiones en el ordenamiento español,* Ed. Dykinson, Madrid, España, 2018, p. 160.

[28] También señala que "la regulación debería centrarse en incentivar eficazmente un comportamiento justo y jurídico de los operadores (emisores, inversores, mediadores y público en general) más allá de los intereses privados en el mercado". En todo caso, el contrato inteligente siempre hará exactamente lo que dice en su código, pero es probable que el contrato entre las partes incluya obligaciones más allá del propio código.

En escenarios donde aparezcan proyectos de *big data*; la ética, la responsabilidad activa, transparencia y seguridad serán fundamentales en cualquier proyecto. En *big data*, la regulación actual tiene por objeto último evitar la *discriminación* y garantizar la libertad dando primacía a la dignidad del paciente o consumidor y al cumplimiento normativo. Por otro lado, conseguir cierta transparencia en la información a los titulares de los datos, no siempre es posible, ya que a veces no conoce (desde el momento cero) el alcance del proyecto *big data* y sus finalidades. Por ello, podría ser recomendable proponer un nuevo concepto de consentimiento: el consentimiento amplio, de exclusión y dinámico orientado sobre todo para investigaciones científicas. Los individuos deberán tener acceso a sus perfiles, a sus fuentes y a la lógica de la toma de decisiones. Lo más sensible no es tanto el contenido sino las inferencias que se pueden producir. Y es que uno de los mayores problemas de *big data*, por no decir el principal, tiene que ver con la anonimización y el riesgo de reidentificar mediante inferencias, o por vinculación o con otros paquetes de datos personales.

Y en escenarios donde existan proyectos de *blockchain* (sanitario), deberemos prestar especial atención a la identificación del responsable de tratamiento, a la aplicación del derecho de supresión, la limitación del periodo de conservación y la cadena de suministro (subcontrataciones y *smart contracts*). Como medidas a tomar desde el momento inicial del sistema o proyectos, se recomienda a los desarrolladores que no almacenen los datos transaccionales dentro de una cadena de bloques y que se realicen evaluaciones de impacto (EIPD) respecto a las claves públicas. Las soluciones están en la propia tecnología.

Desde mi punto de vista, las soluciones más acertadas se encontraban en torno a las *off-chain,* y *side-chain y middleware.* Los problemas no son de carácter tecnológico sino más bien de cultura de privacidad de los participantes y del reto social de espíritu de comunidad y confianza desde los consorcios sanitarios.En definitiva, el principio de limitación de finalidad del tratamiento de datos, en el caso de *big data*, o la naturaleza inmutable y descentralizada, en el caso de *blockchain*, pueden complicar el acercamiento al absoluto cumplimiento normativo.

Las posibles soluciones que se presentarán en el futuro serán soluciones parciales para casos específicos, flexibles y diferentes a lo que venían conociendo los desarrolladores tecnológicos.El desarrollo tecnológico propiciará soluciones que ya están siendo estudiadas por grupos de trabajo de investigación académicos y por autoridades de control nacionales de protección

de datos. Y todo ello será posible sin hacer retroceder a la innovación y al desarrollo de una sociedad saludable y su investigación biomédica.

Blockchain incluso puede llegar a presentarse con una suerte de facilitador "prioritario" para el propio cumplimiento normativo (del RGPD) tal y como estableció en su momento el CNIL[29] francés. Además, como se señala en el documento elaborado por el Parlamento Europeo (2019) "la cadena de bloques puede ayudar a promover algunos de los objetivos del RGPD". Por tanto, aparece algo nuevo y anecdótico característico del escenario dinámico y disruptivo en el que nos encontramos: la tecnología puede permitir (y ayudar) al cumplimiento normativo.

5. Referencias

Aepd. *Orientaciones y garantías en los procedimientos de anonimización de datos personales.*

Aepd e isms forum spain. *Código de buenas prácticas en protección de datos para proyectos de Big Data,* 2017, pp 29.

Autoridad Catalana de Protección de Datos (APDCAT). *El encargado de tratamiento en el Reglamento General de Protección de Datos (RGPD).*

European Data Protection Supervisor (EDPS). *Annual Report,* 2016.

Benchouf, M. / Ravaud, P., Blockchain technology for improving clinical research quality. *BMC Trialsjournal*. 2017, COUD SECURITY ALLIANCE (CSA). *Expanded Top Ten Big Data Security and Privacy Challenges.*

Cnil. *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, 2018.

Comité Internacional de Bioética. *Informe del IBC sobre big data y salud.*

European Parliament. *Blockchain and the Data General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*

Fink, M., "Blockchains y Protección de datos en la Unión Europea", *Der Juristiche Verlag Lexxion,* Núm. 1, Vol. 4, 2018.

Giannopolou, A. / Ferrari, V., Distributed Data Protection And Liability On Blockchains. *INTERNET SCIENCE. 5th International Conference, INSCI 2018*. St.Petersburg, Russia, October 24-26, Proceedings, Vol. 2. Workshops, 2018.

González-Meneses, Manuel, *Entender Blockchain: Una introducción a la Tecnología de Registro Distribuido,* Ed. Thomsons Reuters Aranzadi, 2017.

Gt29. *Dictamen 03/2013 sobre la limitación de la finalidad*. (WP 203).

Hartzog, Woodrow / Stutzman, Frederic D., "Obscurity by Design*", Washington Law Review,* Vol. 88, 2013.

[29] CNIL, *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 2018.* Disponible en: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data [Última consulta: 10 de septiembre de 2019].

Ibañez Jimenez, J. Wenceslao, *Blockchain: Primeras cuestiones en el ordenamiento español,* Ed. Dykinson, 2018.

Mertz, M. / Jannes, M. / Schlomann, A. / Manderscheid, E. / Rietz, C. / Woopen, C. *Digitale Selbstbestimmung* Centro de Ética, Derechos, Economía y Social de Colonia Ciencias de la Salud, 2016.

Martínez Martínez, Ricard, "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", *Revista Valenciana d'Estudis Autonòmics*, Núm. 62, 2017.

Nuffield Council on Bioethics, *La recopilación, vinculación y uso de datos en biomedicina investigación y cuidado de la salud: cuestiones éticas*.

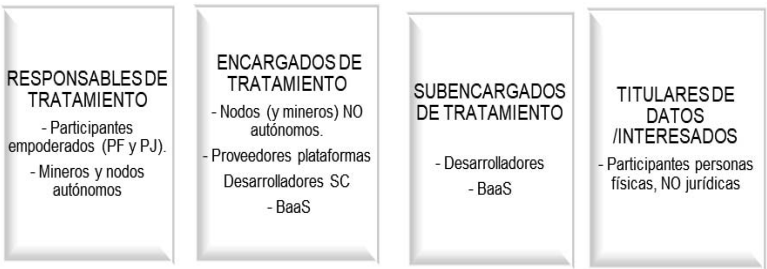
Tabla I. Fases y Códigos de buenas prácticas en protección de datos para proyectos *Big Data*. Fuente: AEPD e ISMS Forum España[30].

Fase *Big Data*	Estrategia	Implementación
Adquisición y recolección	Minimizar Agregar Ocultar Informar Controlar	Seleccionar antes de adquirir Evaluaciones de Impacto (EIPD) Anonimización en la fuente origen Transparencia-comunicación del interesado Mecanismos para recabar consentimiento
Análisis y validación	Agregar Ocultar	Técnicas de anonimización Herramientas de cifrado
Almacenamiento	Ocultar Separar	Herramientas de cifrado Mecanismos de autenticación y control de acceso. Almacenamiento distribuido/ descentralizado
Explotación	Agregar	Técnicas de anonimización
Todas las fases	Cumplir/ demostrar	Definición de políticas Trazabilidad de las acciones Herramientas de cumplimiento

[30] AEPD e ISMS Forum Spain, *Código de buenas prácticas en protección de datos para proyectos de Big Data*, 2017, pp 29. Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (Ver también http://www.agpd.es y http://www.ismsforum.es.)

Tabla II. Posible esquema de "ecosistema" de *blockchain* sanitario formados por diferentes participantes. Fuente propia.

Tabla III. Esquema de sujetos jurídicos en *Blockchain* de la Industria del cuidado de la salud. Fuente propia.



Análisis doctrinal y jurisprudencial de los delitos de descubrimiento y revelación de secretos en el ámbito sanitario*

Doctrinal and jurisprudential analysis of the crimes of discovery and revelation of secrets in the health field

Iker Conal Fuertes

Investigador Predoctoral en el Grupo de Investigación Cátedra de Derecho y Genoma Humano

Universidad del País Vasco UPV/EHU (Bilbao, España)

DOI: 10.14679/1150

Sumario / Summary: 1. Introducción. 2. Régimen jurídico en España: artículos 197 a 201 del Código Penal. 2.1. Antecedentes históricos. 2.2. El bien jurídico protegido (I): la intimidad. 2.3. El bien jurídico protegido (II): los datos de carácter personal reservados. 2.4. Breve referencia a las modificaciones derivadas de la reforma del

* Artículo recibido el 18 de junio de 2019 y aceptado para su publicación el 10 de julio de 2019.

Este artículo ha sido posible gracias al Proyecto de Investigación BIGDATIUS (Uso de datos clínicos ante
nuevos escenarios tecnológicos y científicos -*Big Data*-. Oportunidades e implicaciones jurídicas. UPV/EHU. Ref.: DER2015-68212-R), financiado por el Ministerio de Economía y competitividad y Fondo Europeo de Desarrollo Regional (FEDER), a la financiación del Gobierno Vasco (ayuda con referencia número IT1066-16, concedida por el Departamento de Educación del Gobierno Vasco para apoyar las actividades de Grupos de Investigación del Sistema Universitario Vasco) y del Instituto de Salud Carlos III
de Madrid (proyecto de investigación PMP15/00007 Functional and Clinical Impact of the Genome Analysis in CLL, integrado en el Plan Estatal de I+D+i cofinanciado por el ISCIII - Subdirección General de Evaluación y el Fondo Europeo de Desarrollo Regional FEDER - "Una manera de Hacer Europa").

año 2015. 3. Artículo 199.2: el delito de divulgación de secretos profesionales. 3.1. El médico como profesional obligado al sigilo. 3.2. Principales características de este delito. 3.3. Concursos. 4. Causas de exclusión del secreto profesional. 4.1. Estado de necesidad. 4.2. Cumplimiento de un deber. 5. Análisis jurisprudencial. 6. Conclusiones. 7. Bibliografía.

Resumen / Abstract: La protección de la intimidad y de los datos personales reservados es una de las bases fundamentales de la relación entre médico y paciente. A pesar de ello, en ocasiones, los facultativos transmiten a un tercero los datos contenidos en la historia clínica incurriendo en un delito perseguible desde el derecho penal. Este artículo comienza analizando los artículos 197 a 201 del Código Penal español para contextualizar la materia a tratar y otorgar una visión amplia de esta modalidad delictiva, y se centra después en el artículo 199.2 del mismo texto legal por ser el que, de manera específica, se aplica a los profesionales sanitarios obligados al sigilo que incurren en dicha conducta. Además, se hace una útil mención a aspectos prácticos como el alcance del secreto profesional del médico o las causas de exclusión del mismo. Por último, se analiza la jurisprudencia existente en relación con la cuestión, a pesar de su escasez. El presente artículo pretende servir por igual a profesionales del derecho y de la medicina para comprender más en profundidad, siempre desde la perspectiva del derecho penal, el descubrimiento y revelación de secretos en el ámbito sanitario.

The protection of privacy and private personal data is one of the cornerstones of the physician-patient relationship. In spite of this, doctors sometimes transmit the data contained in the medical history to a third party, thereby committing a crime that can be prosecuted under criminal law. This article begins by analysing articles 197 to 201 of the Spanish Criminal Code in order to contextualize the matter to be dealt with and give a broad view of this type of crime. It then focuses on article 199.2 of the same legal text because it is the one which specifically applies to health professionals forced to secrecy who engage in such conduct. In addition, it includes a useful mention of practical aspects such as the scope of the physician's professional secrecy or the causes of exclusion from it. Finally, it analyses the existing jurisprudence in relation to the issue, despite its scarcity. This article aims to serve law and medicine professionals alike to understand more deeply, always from the perspective of criminal law, the discovery and disclosure of secrets in the health field.

Palabras clave / Keywords:

Delitos / Descubrimiento / Revelación / Divulgación / Secretos / Profesionales / Sanitarios.

Crimes / Discovery / Disclosure / Dissemination / Secrets / Professionals / Healthcare.

1. Introducción

El concepto de *secreto*, entendido como información cuidadosamente reservada y oculta, adquiere una trascendencia mayor en el ámbito sanitario, puesto que supone una garantía de protección de la esfera más íntima de las personas en su momento de mayor vulnerabilidad: aquel en que padecen una enfermedad.

Cuando una persona acude a un facultativo, espera no solo que examine desde un punto de vista profesional los signos y síntomas perceptibles ofreciendo después un tratamiento o distintos tratamientos alternativos. En nuestro tiempo, esto es solo el mínimo exigible. El paciente espera, además, un trato empático y correcto, la observancia de los principios bioéticos y, por supuesto, el estricto cumplimiento de la legalidad por parte del profesional. De manera que, centrándonos en este último elemento, ¿qué sucede cuando el paciente y el profesional sanitario entran en contacto y tiene lugar una transmisión de información del primero al segundo (ya sea a través de lo referido por el propio paciente, o se derive de las observaciones del primero)? ¿Hasta qué punto se encuentra protegida esa información? ¿Puede un paciente o un grupo de pacientes iniciar acciones legales si entienden que ha habido un uso incorrecto de la misma? ¿Puede hacerlo la Fiscalía, actuando *motu proprio*?

A lo largo de los años, diversos autores[1] han analizado el marco jurídico existente para la protección de la información contenida en la historia clínica de los pacientes, abordando la cuestión desde la perspectiva del derecho penal. Antes de añadir a esta tradición mi modesta aportación, quisiera destacar dos aspectos que considero esenciales en relación con este tema. En primer lugar, la incidencia de la reforma del Código Penal en el año 2015, que si bien no tuvo efectos sobre determinados artículos (como el 198), sí alteró profundamente otros (como el 197, que vio modificada, incluso, su estructura). Estas modificaciones, a mi juicio, deben ser analizadas y tenidas en cuenta, especialmente en lo que respecta a la valoración de la jurisprudencia previa a la fecha de la reforma. En segundo lugar, la importancia del tipo de datos que el legislador intenta proteger. Será en apartados posteriores cuando analizaré la adecuación o no de las penas a los delitos, y el bien jurídico protegido. En

[1] Destaca la obra de Romeo Casabona, Carlos María, *Los delitos de descubrimiento y revelación de secretos: especial consideración a su comisión en conexión con las nuevas tecnologías de la información y de la comunicación,* Ed. Tirant lo Blanch, Valencia, España, 2005, 220 pp. y a un nivel más específico (el de los datos genéticos), la aportación de Nicolás Jiménez, Pilar, "La protección de los datos genéticos de carácter personal en Derecho penal español: un caso práctico", *Temas de Derecho penal: libro homenaje a Luis Guillermo Cornejo Cuadros,* Armaza Armaza, Emilio José / Mendoza Valdez, José / De Miguel Beriain, Iñigo / Urruela Mora, Asier (Coords.), Ed. Adrus, Arequipa, Perú, 2008, pp. 189-202. Además, hay que mencionar la monografía de Rueda Martín, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Ed. Atelier, Barcelona, España, 2018, 248 pp., en la que la autora realiza un magnífico análisis de los delitos comprendidos en los artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198 del Código Penal, al tiempo que reflexiona acertadamente sobre el efecto que ha tenido en la vida privada de los ciudadanos la progresiva implantación de las nuevas tecnologías de la información y la comunicación.

esta introducción, en cambio, quiero poner de manifiesto la trascendencia de la información que se busca proteger. Y es que, sin apartarnos nunca de la perspectiva penal, está claro que, a juicio de los expertos[2], la introducción del nuevo Reglamento General de Protección de Datos (2016) ha supuesto un intento de dar una respuesta preventiva y sancionadora dotada de eficacia y eficiencia a ciertas conductas no responsables o frente a prácticas ilícitas que pudiesen afectar a los datos personales.

Si a esto añadimos el desarrollo por parte de la Unión Europea de legislación como la Directiva sobre seguridad de las redes y de los sistemas de información de la Unión (2016), orientada a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la misma, se pone de manifiesto su interés en coordinar a los Estados miembros en la lucha contra los ciberdelitos. No podía ser de otra manera, dado el impacto de los medios, plataformas y entornos digitales sobre la protección de datos, toda vez que al operarse de manera mayoritaria a través de la red (o de las redes) utilizando tecnologías de la información y la comunicación (TIC) se puede prácticamente asegurar la proyección y la difusión inmediata de los mismos. En la actualidad, la utilización indebida de una información de carácter sensible obtenida mediante métodos ilegales es doblemente peligrosa, puesto que su propagación masiva es técnicamente posible, procedimentalmente sencilla y, sobre todo, muy difícil de perseguir utilizando el derecho penal de un país en particular, a causa de la posible naturaleza internacional del delito.

Es en este contexto donde debemos encuadrar nuestro análisis, sin perder nunca de vista el desarrollo histórico del tratamiento que el ordenamiento jurídico español ha otorgado a estos delitos. Teniendo en cuenta la tendencia legislativa cada vez más restrictiva de la Unión Europea, puede aventurarse un futuro endurecimiento en la persecución a los mismos. No obstante, la jurisprudencia existente en la actualidad se ha venido desarrollando con base en la redacción del Código Penal, tanto antes como después de la reforma del año 2015. Sirva esta introducción, en consecuencia, no tanto para valorar el actual estado de las cosas a nivel estatal, sino para evidenciar la enorme trascendencia que se otorga a nivel comunitario a la protección de datos, y para prever[3] la manera en que esto afectará a las herramientas con las que

[2] Dopazo Fraguío, Pilar, "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (novedades del Reglamento General de Protección de Datos)", *Revista española de derecho europeo,* Núm. 68, 2018, pp. 113-148.

[3] De la Mata Barranco, Norberto Javier, *Derecho Penal europeo y legislación española: las reformas del Código Penal,* Ed. Tirant lo Blanch, Valencia, España, 2015, 251 pp. Este

contamos actualmente para castigar a quienes pretendan hacerse con ellos infringiendo el derecho de los pacientes a preservar su intimidad.

2. Régimen jurídico en España: artículos 197 a 201 del Código Penal

El Libro II, Título X (Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio), Capítulo Primero (Del descubrimiento y revelación de secretos) de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, recoge los artículos 197 a 201. En este apartado, dedicado al análisis crítico de la propia legislación, es mi intención, basándome en los sólidos fundamentos de la doctrina[4], exponer los artículos que afectan a los profesionales sanitarios de manera ordenada, con un enfoque útil y práctico que permita su adecuada comprensión tanto a estos como a los juristas.

2.1. Antecedentes históricos

La primera mención al delito de infracción del deber del secreto profesional se encuentra en el Código Penal de 1822, en cuyo artículo 424 se especificaba que, entre otros profesionales, los médicos y cirujanos que revelasen un secreto que les hubiese sido confiado por razón de su estado, empleo o profesión fuera de los casos permitidos por la ley sufrirían un arresto de dos meses a un año y pagarían una multa de treinta a cien duros. Si el secreto revelado fuese susceptible de causar a la persona que lo confió alguna responsabilidad criminal, alguna deshonra, odiosidad, mala nota o desprecio en la opinión pública, habría que sumar a la multa mencionada la pena de reclusión de uno a seis años. En caso de haber mediado soborno, se impondría, con carácter adicional, la pena de infamia al sobornado, no pudiendo volver a ejercer su profesión u oficio.

---

libro analiza la adecuación de las reformas del Código Penal a las distintas directivas y decisiones marco de la Unión Europea. Al destacar los posibles déficits de cumplimiento, los excesos y las contradicciones, es una herramienta muy útil para valorar, en casos similares al que nos ocupa, la influencia que está teniendo la legislación comunitaria en nuestro Código Penal a lo largo del proceso de consolidación de la Unión Europea.

[4] Romeo Casabona, Carlos María, *Las transformaciones del Derecho Penal en un mundo en cambio (Volumen I),* Ed. Adrus, Arequipa, Perú, 2004, pp. 339-370. El tiempo ha dado la razón al autor, puesto que hace más de una década señalaba, en su valoración final de las penas previstas para esta clase de delitos, que existía una conciencia social entonces escasa en relación con la necesidad de respetar el deber de secreto, pero que existiría un aumento paulatino de la misma. A la luz de lo expuesto con anterioridad, es evidente que esta conciencia social no solo ha aumentado, sino que se ha generalizado.

El hecho de que el legislador introduzca un *numerus clausus* (una enumeración cerrada de los profesionales que podrían incurrir en el delito) será importante, dado que, continuando con esta costumbre, en el Código Penal de 1848 ya no se menciona de manera específica al médico ni al cirujano, aunque sí al funcionario público (artículo 378), en una tradición que se mantendría hasta nuestros días (salvo por un breve inciso histórico derivado del artículo 683.2 del Código Penal de 1928 en el que el tipo delictivo era muy amplio, pues se basaba en la divulgación de los secretos de otro sin importar cómo se hubiesen conocido). Hay que mencionar, aunque sea de manera anecdótica, los distintos proyectos, anteproyectos y borradores del Código Penal desarrollados durante los años ochenta y noventa, cuyas redacciones en relación con la tipificación penal de la vulneración del secreto profesional pueden considerarse deficientes.

La aprobación del Código Penal del año 1995 permitió la incorporación de estos delitos al derecho penal español en el Libro, Título y Capítulo anteriormente expuestos.

2.2. El bien jurídico protegido (I): la intimidad

Centrándonos en la legislación vigente[5], el bien jurídico protegido en los delitos del Capítulo Primero es difícil de delimitar puesto que, siendo su eje central la intimidad, va más allá de la misma y ampara los datos reservados de carácter personal y familiar.

La intimidad serían aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven involucrados terceros, entendiendo por tales tanto los particulares como los poderes públicos. Se trata de un derecho inherente de la personalidad, reforzado como derecho fundamental (artículo 18 de la Constitución Española) e, incluso, como un derecho humano (artículo 12 de la Declaración Universal de los Derechos Humanos), trascendiendo al ejercicio de otros derechos públicos o privados. A pesar de esto, la intimidad tiene un carácter difuso, y

[5] Romeo Casabona, Carlos María, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", Romeo Casabona, Carlos María / Sola Reche, Esteban / Boldova Pasamar, Miguel Ángel (Coords.), *Derecho Penal, Parte Especial,* Ed. Comares, España, 2016, pp. 254-286. Las personas que necesiten profundizar en esta clase de delitos encontrarán un análisis minucioso de los mismos en sus páginas.

en ocasiones, como veremos más adelante, el individuo puede verse obligado a compartir parcelas de la misma[6].

No obstante, con el aumento de los medios técnicos de captación y transmisión de la imagen y del sonido, así como de acumulación y procesamiento de la información en general y de los datos de carácter personal en particular, crecieron también los procedimientos susceptibles de vulnerar la intimidad. El alcance de la esfera íntima de los individuos ha disminuido progresivamente a causa de los profundos cambios en las relaciones sociales derivadas de la creciente utilización de la tecnología. Además, tanto los poderes públicos como el sector privado recaban cada vez más información en relación con los ciudadanos, argumentando que esto permitirá un cumplimiento más efectivo de sus funciones. En una sociedad avanzada y, por ende, compleja, la intimidad puede adquirir distintas manifestaciones, afectando a bienes jurídicos próximos pero diferentes[7].

2.3. El bien jurídico protegido (II): los datos de carácter personal reservados

En ocasiones, el sujeto debe aportar información personal de carácter privado e, incluso, reservado, viéndose obligado a que se archive o procese por terceras personas (haya sido suministrada o no por él). En estos casos, también se le reconoce al individuo cierta capacidad en relación con dicha información. Puede desgajarse un bien autónomo de la intimidad, que no siempre se verá afectada. En efecto, los derechos antes conocidos como ARCO (de acceso, rectificación, cancelación y oposición), que en la nueva normativa[8] han pasado a ser derechos ARCOPOL (de acceso, rectificación, cancelación, oposición, portabilidad, olvido y limitación del tratamiento), amparan al individuo, tengan los datos carácter íntimo o no. Sirva como ejemplo el tipo delictivo del artículo 197.2, relativo a la modificación o alteración de datos que pueden no afectar a la intimidad. El Código Penal, por lo tanto,

---

6 Romeo Casabona, Carlos María, *op. cit.,* p. 255.

7 Romeo Casabona, Carlos María, *op. cit.,* pp. 255-257.

8 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). Algunos profesionales hablan, en cambio, de derechos ARSOPOL, puesto que la cancelación ha dejado paso a la supresión, de manera que el acrónimo también debería cambiar respecto al original. Es cierto que en el texto del Reglamento no se hace referencia a la cancelación, y sí a la supresión (artículo 17), de manera que, desde un punto de vista técnico, el acrónimo ARSOPOL sería más adecuado. No obstante, parece haberse impuesto mayoritariamente, al menos de momento, el acrónimo ARCOPOL.

puede ser utilizado para amparar esta clase de datos personales, tengan o no la consideración de íntimos, siempre que gocen del carácter de reservados.

2.4. Breve referencia a las modificaciones derivadas de la reforma del año 2015

La Ley Orgánica 1/2015, de 30 de marzo, por la que se modificaba la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, introdujo una serie de novedades en relación con esta clase de delitos, siendo el artículo más afectado el 197. Los artículos 198, 199, 200 y 201, por su parte, no sufrieron modificación alguna.

En lo que respecta al artículo 197, la nueva Ley Orgánica supuso un notable cambio en su redacción que fue desde las meras correcciones estilísticas (la coma en lugar de la letra "o" del 197.1) a las modificaciones de buena parte del artículo (partición del 197.5 en distintos subapartados para dotar de mayor claridad al conjunto, sin alteración de su contenido salvo por la introducción de un subapartado "b", que castiga la comisión de los hechos mediante la utilización no autorizada de datos personales de la víctima), pasando por el traslado de contenido de la redacción anterior del propio artículo a los nuevos artículos 197 bis, 197 ter, 197 quater y 197 quinquies (por ejemplo, el nuevo artículo 197 quater dio acomodo a lo que antes se regulaba en el artículo 197.8: la aplicación de las penas superiores en grado en caso de comisión de los hechos por en el seno de una organización o grupo criminal[9]). Estas modificaciones aportan claridad al conjunto y facilitan la labor del jurista pero, en mi opinión, no resuelven algunos problemas de fondo que señalaré en el análisis de este artículo, que realizo a continuación.

Retomando por un momento lo expuesto en la introducción de este artículo, resulta fundamental la conexión que han realizado algunos autores[10] entre esta reforma y la incorporación de la Directiva 2013/40/UE,

---

[9] Escuchuri Aisa, Estrella, "Comisión de delitos en el marco de organizaciones y grupos criminales. Algunos problemas que plantea la regulación del Código penal español en relación con la delincuencia organizada", *Revista Aranzadi de Derecho y Proceso Penal,* Núm. 37, 2015, pp. 133-176.

[10] Obispo Triana, Concepción, "Circular 3/2017, de 21 de septiembre, sobre la reforma del código penal operada por la LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos", *Revista Aranzadi Doctrinal,* Núm. 10, 2017, pp. 183-192. La autora expone de manera ordenada las novedades introducidas en el Código Penal por la modificación, como la nueva circunstancia agravatoria del artículo 197.4.b) o la nueva figura delictiva del artículo 197.7. Además, su aportación incluye útiles explicaciones aclaratorias que profundizan en la manera en

relativa a los ataques contra los sistemas de información. Entre sus objetivos encontramos la pretensión de establecer unas normas mínimas comunes para todos los Estados en la definición de las infracciones penales y las sanciones aplicables, así como reforzar y mejorar la cooperación entre las autoridades competentes. Haciendo mención específica a los delitos de descubrimiento y revelación de secretos, la Directiva buscaba ofrecer respuesta penal ante los comportamientos relacionados con la divulgación de imágenes o grabaciones de una persona contra su voluntad que pudiesen afectar a su intimidad personal. A pesar de esto, la rapidez con la que tiene lugar la evolución tecnológica se traduce en nuevos riesgos y amenazas, obligando a articular nuevas figuras delictivas y a modificar las existentes para poder actuar desde un punto de vista penal, haciendo frente así a nuevas situaciones que, por su gravedad y por los riesgos que generan, así lo requieren. Para ello, el texto legal instaba a los Estados a la tipificación penal de nuevas conductas y al establecimiento correlativo de penas efectivas, proporcionadas y disuasorias que contemplasen agravantes con base en circunstancias como los daños causados. En lo que respecta a la definición de los tipos penales, tomaba como punto de partida los artículos 2 a 6 del Convenio de Budapest sobre ciberdelincuencia. El objetivo de la Directiva era el uso seguro del ciberespacio en el que se garantizasen los derechos de todos los ciudadanos, así como la protección de organismos e instituciones públicos y privados y de los propios Estados.

La versión del articulado que utilizo para llevar a cabo el análisis en el subapartado siguiente es la actualizada, pero sirva esta breve exposición sobre las modificaciones para tenerlas en cuenta al valorar la jurisprudencia de los años anteriores a la reforma de 2015, así como para comprender la motivación existente tras la misma, cuyo origen radica en las exigencias derivadas de la legislación comunitaria para nuestra norma penal estatal.

3. Artículo 199.2: el delito de divulgación de secretos profesionales

Los artículos 197, 197 bis, 197 ter, 197 quater y 197 quinquies son muy interesantes desde un punto de vista jurídico-penal para valorar de forma general las conductas que pretende castigar el legislador y contextualizar esta clase de delitos. No obstante, para analizar de manera específica las consecuencias de que un profesional sanitario divulgue secretos en relación

que se han alterado los artículos aquí tratados respecto a la versión del texto legal previa a la reforma.

con los cuales tenga una obligación de sigilo o reserva, debemos centrarnos en el artículo 199.2. En su redacción actual dice así: "El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años".

Hay que realizar una primera matización[11] en relación con el artículo 199, dado que tipifica conductas distintas. Su apartado primero (artículo 199.1) castiga la revelación de los secretos que hayan sido conocidos por el sujeto por razón del oficio que ejerza, o bien como consecuencia de la relación laboral en la que sea parte. El párrafo segundo (199.2), por su parte, castiga específicamente la violación del secreto profesional, entendido como el incumplimiento de deberes derivados del ejercicio de una profesión que conlleva la obligación o deber de reserva o sigilo respecto a la información que se posea de otra persona[12]. No debemos olvidar que el propio juramento hipocrático incluía, en el año 500 antes de Jesucristo (a pesar de que su fecha exacta sigue siendo objeto de disputa), la siguiente frase, que podemos relacionar fácilmente con el tipo delictivo: "Todo lo que vea y oiga en el ejercicio de mi profesión, y todo lo que supiere acerca de la vida de alguien,

---

[11] Fernández Pantoja, Pilar, "El delito de revelación y divulgación de secretos en el ámbito sanitario", *Estudios jurídicos sobre responsabilidad penal, civil y administrativa del médico y otros agentes sanitarios,* Ed. Dykinson, Madrid, España, 2010, pp. 287-321. La autora se remite a la opinión de Romeo Casabona para diferenciar entre los apartados primero y segundo del artículo 199. Atendiendo a la misma: *"La diferencia entre ambos tipos delictivos descansa precisamente en la divergente naturaleza de la actividad ejercida por los sujetos activos del respectivo delito, en todo caso relacionada con el trabajo: en el primer caso (artículo 199.1), el sujeto activo realiza prestaciones laborales, normalmente por cuenta ajena, sin el respaldo de un título académico u oficial, lo que sí ocurre en el segundo (artículo 199.2), con independencia de que presente sus servicios de forma autónoma o por cuenta ajena y de que desempeñe en sentido estricto una actividad laboral"* (cita extraída por la autora de Romeo Casabona, Carlos María, *Comentarios al Código Penal, Parte Especial, Volumen II,* Díez Ripollés, José Luís / Romeo Casabona, Carlos María, *et ál* (Coords.), Ed. Tirant lo Blanch, Valencia, España, 2004, p. 817).

[12] Suárez-Mira rodríguez, Carlos / Judel prieto, Ángel / Piñol Rodríguez, José Ramón, *Manual de Derecho Penal. Parte Especial,* Ed. Aranzadi, Cizur Menor, España, 2011, 760 pp. Los autores sostienen, en lo concerniente a la diferenciación entre ambos artículos: "La singularidad de este precepto deriva no tanto de la conducta típica como del ámbito en el que se produce la transgresión del deber de privacidad. La revelación o divulgación ha de acontecer en la esfera de las relaciones de trabajo, diferenciándose en que mientras que en el párrafo primero el sujeto activo puede ser cualquier persona que por razón del oficio que desempeñe o de las relaciones laborales que le unan con el sujeto pasivo tenga conocimiento del secreto que posteriormente revela, en el párrafo segundo ha de ostentar la condición de profesional; por lo tanto, debe hallarse en posesión de título académico u oficial […]".

si es cosa que no debe ser divulgada, lo callaré y lo guardaré con secreto inviolable". A un nivel más profundo, es fascinante comprobar cómo el tema a tratar se relaciona íntimamente con lo dispuesto en el juramento. Aunque en su encabezamiento se comete el profundo error de jurar por falsos dioses paganos, en lugar de depositar su fe el facultativo en el Dios de los Cristianos, dice así: "Jamás daré a nadie medicamento mortal, por mucho que me soliciten, ni tomaré iniciativa alguna de este tipo; tampoco administraré abortivo a mujer alguna. Por el contrario, viviré y practicaré mi arte de forma santa y pura". Más adelante, haré referencia a un caso en el que la modificación de varias historias clínicas fue utilizada, incluso, para que se cumpliesen los requisitos legales necesarios para practicar abortos, permitiendo que unos médicos indignos de tal nombre se aprovechasen de estas maquinaciones criminales.

Centraré mi análisis en el apartado segundo (artículo 199.2), relativo a la violación del secreto profesional, orientándolo siempre al ámbito sanitario. El fundamento político-criminal[13] de este delito se sustenta sobre la persona que se ve en la necesidad de acudir a un profesional (en este caso, el médico), viendo limitada por las circunstancias la preservación de su intimidad. Dicha limitación conlleva una accesibilidad del facultativo a la vida privada ajena, y es ahí donde se fundamenta el secreto profesional como deber jurídico, y no únicamente ético-profesional. La profesión médica tiene como uno de sus presupuestos el acceso a la intimidad de los pacientes, generándose un especial deber de sigilo. Los ciudadanos corrientes, por su parte, no están vinculados a esta obligación jurídica. El ordenamiento jurídico es más exigente con el facultativo quien, para llevar a cabo su trabajo de forma adecuada, requiere el conocimiento lícito de la intimidad de sus pacientes, renunciando estos de forma relativa a su intimidad presuponiendo la lealtad del profesional, y dando por sentado que los datos o las informaciones personales quedarán preservados y serán tratados con un nivel de confidencialidad adecuado.

3.1. El médico como profesional obligado al sigilo

El médico encaja en la figura del confidente necesario. Su obligación de sigilo o reserva no se deriva, no obstante, del hecho de que su profesión tenga una notable relevancia social, sino de que el paciente tiene necesariamente que transmitirle información privada para que pueda cumplir con su

[13] García Albero, Ramón, *Comentarios al Código Penal (Tomo II),* Ed. Aranzadi, Cizur Menor, España, 2008. La información incluida forma parte de su "Comentario al artículo 199 del Código Penal".

desempeño profesional (lo mismo sucede, por ejemplo, con los psicólogos). El artículo 199.2 no establece un *numerus clausus*, sino que opta por un sistema de cláusula general en relación con los posibles sujetos activos del delito. A pesar de esto, podemos estar seguros de que los profesionales de la medicina son confidentes necesarios, dado que reúnen los dos requisitos establecidos para ello.

En primer lugar, el carácter necesario de los servicios profesionales que ofrece genera una esfera de confidencialidad que da lugar al deber de sigilo. En segundo lugar, este deber de sigilo es de tipo jurídico (es decir, está instituido por normas legales o reglamentarias generales de carácter estatal, no contemplando el tipo delictivo perseguir la mera indiscreción). Así lo evidencian el artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad, al reconocer a los pacientes el derecho a la confidencialidad en el ámbito de la prestación de servicios sanitarios, y el artículo 16.6 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que obliga al personal que acceda a los datos de la historia clínica en el ejercicio de sus funciones al deber de secreto. El artículo 7.1 del mismo texto legal garantiza el derecho de toda persona a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin una autorización amparada por la Ley.

En último lugar, a un nivel más genérico, pero revestida de enorme importancia, está la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuyo artículo 5 regula el deber de confidencialidad que vincula a todas las personas que intervengan en cualquier fase del tratamiento de datos, siendo esto complementario de los deberes de secreto profesional. A esto hay que añadir el Código de Ética y Deontología Médica de 1978 (actualizado por última vez en 2011), que además de hacer referencia en distintos artículos a la confidencialidad, especifica en su artículo 27.7 el deber del médico de preservar en su ámbito social, laboral y familiar la confidencialidad de los pacientes, al tiempo que consagra (artículo 27.1) el secreto médico como uno de los pilares en los que se fundamenta la relación médico-paciente.

3.2. Principales características de este delito

De acuerdo al artículo 199.2 del Código Penal, para que se verifique un delito de revelación de secreto profesional será necesario que el sujeto activo sea un profesional que incumpla la obligación de sigilo o reserva, que

se divulguen secretos y que estos hayan sido conocidos de manera lícita en el desarrollo del ejercicio de la profesión[14]. La redacción[15] del tipo exige la existencia de un acceso lícito (y, por lo tanto, consentido) en la intimidad ajena seguido de un segundo comportamiento con relevancia penal: la revelación o divulgación de lo que lícitamente se ha conocido. Ya hemos visto en el apartado anterior que el médico está obligado a garantizar, salvo en casos muy específicos, la confidencialidad de sus pacientes, de manera que, aplicando los requisitos genéricos al ámbito sanitario, se trataría del facultativo que, habiendo conocido de manera lícita en el desarrollo del ejercicio de su profesión un secreto, procediese a divulgarlo.

Así, la acción típica consistirá en divulgar los secretos de otra persona, incumpliendo con ello las obligaciones profesionales de sigilo o reserva. El objeto material del delito es el secreto ajeno (aquellos aspectos relativos a su propia intimidad que el paciente comparte con el facultativo a fin de obtener sus servicios profesionales).

En cuanto al tipo subjetivo, es necesario el *dolo* en cualquiera de sus formas. El médico debe ser consciente de la naturaleza del secreto, es decir, de su carácter reservado y de su contenido íntimo, y de su obligación de reserva o sigilo.

Para poder perseguir este delito será necesario que el paciente que considere que se han visto vulnerados sus derechos o su representante legal interpongan una denuncia. No obstante, en aquellos casos en que el paciente afectado sea menor de edad, una persona con discapacidad especial necesitada de especial protección o se trate de una persona desvalida, podrá intervenir el Ministerio Fiscal. Estos requisitos no serán de aplicación cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas (en cuyo caso habría que estar a lo dispuesto en el artículo 201.2).

---

14 Caruso Fontán, María Viviana, "La responsabilidad penal de los encargados de bases de datos de ADN frente a la cesión de información contenida en los registros", *Revista de Derecho Penal,* Núm. 40, 2003, pp. 37-63. La autora recalca la importancia de la licitud del acceso a la información en contraposición a la ilegitimidad de la traslación de la misma realizada a terceros.

15 Morales Prats, Fermín, "Reflexiones político criminales sobre los límites de la intervención penal en los delitos contra la privacy (*sic*): la reforma del CP de 2015 (LO 1/2015)", *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo,* Bacigalupo, Silvina / Feijoo Sánchez, Bernardo José / Echano Basaldúa, Juan Ignacio (Coords.), Ed. Universitaria Ramón Areces, España, 2016, p. 1146.

3.3. Concursos

Ya hemos visto la manera en la que el Código Penal prevé el comportamiento del profesional. No obstante, en ocasiones, el profesional, además de serlo, es también un funcionario o autoridad pública, en cuyo caso debemos plantearnos la posibilidad de la existencia de un concurso de normas[16]. Y es que, cuando el sujeto activo tenga esta consideración, no acudiríamos al artículo 199.2, sino a los delitos previstos en el artículo 417, en el que además de tutelar la intimidad (entendida como revelación de secretos o informaciones) se protege, además, el correcto funcionamiento de la Administración Pública. Estaríamos, por lo tanto, ante un delito pluriofensivo. El concurso de normas se resolvería a favor del artículo 417, tomando como base el artículo 8.3 del Código Penal, que recoge el principio de absorción. Al centrarnos en el sector sanitario, no procede analizar otros concursos que podrían darse en otros ámbitos, y sin embargo sí considero importante recalcar que la preferencia en la aplicación de otros delitos respecto al previsto en el artículo 199.2 conduce a una escasa aplicación del mismo.

Aun estando de acuerdo con la solución expuesta a favor del concurso de normas[17], parte de la doctrina[18] recalca la importancia, para poder acudir al artículo 417.2, de que se reúnan todos los requisitos típicos: el sujeto activo debe ser un funcionario o autoridad pública que, por razón de su cargo, tenga conocimiento de secretos o informaciones. Estos secretos deben estar referidos a un particular y, por último, los secretos deben ser divulgados de manera ilícita. Ambos tipos penales son enormemente similares, de manera que el elemento que los diferencia (el sujeto activo funcionario o autoridad) es, al mismo tiempo, lo que determina la resolución del concurso de normas a su favor, al ser ésta más compleja.

Algunos autores[19] han ahondado en el análisis de este artículo 417, permitiéndonos comprender con más detalle el tipo delictivo en el que de-

---

[16] Fernández Pantoja, Pilar, *op. cit.,* pp. 287-321.

[17] Romeo Casabona, Carlos María, *Derecho Penal, Parte Especial. Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de Marzo, op. cit.*, p. 279.

[18] Romeo Casabona, Carlos María, *Comentarios al Código Penal, Parte Especial, Volumen II, op. cit.,* p. 836.

[19] De la Mata Barranco, Norberto Javier, "El funcionario público ante el Derecho Penal", *Revista jurídica de Castilla y León,* Núm. 20, 2010, pp. 17-78. El autor, en la línea de lo expuesto anteriormente, rechaza la idea de que se persiga la mera indiscreción, dejando fuera del precepto hechos confidenciales de menor entidad. Estoy de acuerdo con él y, no obstante, quisiera introducir una pequeña matización. Creo que es muy importante la intencionalidad del sujeto activo a la hora de juzgar qué es información irrelevante y qué no

bemos encuadrar la conducta del sujeto activo con posterioridad al concurso de normas. En el mismo, se contempla la revelación de secretos (o violación

---

lo es. Del deber de castigar la divulgación de información sanitaria objetivamente relevante para la intimidad del sujeto pasivo (por ejemplo, una enfermedad infectocontagiosa en relación con la cual no concurre ninguna de las circunstancias de exclusión del secreto profesional), no me cabe duda. Del mismo modo, y pensando en información que no es tan relevante pero que, aun así, es considerada confidencial, el legislador no puede aspirar a perseguir aquellos comentarios realizados sin mala intención, especialmente los que se derivan de la práctica médica y que son consecuencia del intercambio diario de información inherente a la misma. Lo contrario conduciría a un clima de miedo que, a la larga, sería más perjudicial que beneficioso para la actividad de los facultativos, quienes tendrían que poner un cuidado excesivo en un intercambio de información que debe ser fluido y desarrollarse en un clima interno de confianza (pero también de respeto por el paciente, y en el que impere el sentido común). Y, pese a todo lo anterior, creo que cuando el facultativo revela hechos confidenciales de importancia menor con conocimiento de lo que está haciendo, y además lo hace con la finalidad de perjudicar a un tercero vulnerando su intimidad (o sabiendo que existe la posibilidad de hacerlo), sí debería existir un reproche en el ámbito penal. El desvalor de la acción, por supuesto, sería menor que en el primer ejemplo (de manera que la pena sería también proporcional), pero sí debería actuar la justicia, so riesgo de que la persona afectada se sienta desamparada. El primer elemento a ponderar para realizar una valoración en este sentido es el tipo de información revelada: se trataría siempre de esta información de importancia menor (como, por ejemplo, el resultado de un examen oftalmológico que determina que una persona va a comenzar a llevar gafas, o que un psiquiatra, tras una primera sesión, ha esbozado en la historia clínica sus percepciones en relación con un posible principio de depresión en un paciente). Aunque ambas son notas dentro del historial clínico aparentemente inofensivas por su escasa entidad no son, a mi juicio, iguales. La primera de ellas formaría parte de esa categoría que el autor señala, muy acertadamente, como hechos confidenciales de menor entidad (dado que con su revelación, se haga inconscientemente o con voluntad de perjudicar, el daño es mínimo, puesto que llevar gafas es algo socialmente aceptado que no se traduce en un quebranto para la intimidad del paciente, ni repercutirá de forma negativa en su vida). No sucede lo mismo con estas anotaciones preliminares, con este esbozo basado en una única sesión: su revelación, malintencionada o no, puede conllevar graves consecuencias sociales a nivel laboral o personal a causa de los prejuicios existentes en relación con las patologías mentales. Hasta aquí, la valoración sobre el tipo de información revelada. Lo segundo a tener en cuenta es, reitero, la intencionalidad. Si aceptamos como válida la existencia de determinada información como lesiva (pese a su aparente inocuidad) para el bien jurídico protegido, queda determinar en qué casos será perseguible la actuación del sujeto activo. Pues bien, considero que solo deberían perseguirse las vulneraciones cuando el facultativo actúe con intención de vulnerar el derecho a la intimidad del paciente (entiéndanse como tales, por ejemplo, venganzas personales, o cualquier otro hecho susceptible de ser demostrado con pruebas objetivas frente al juzgador). En todos los demás casos, incluso tratándose de información de la segunda categoría, la actuación del profesional sanitario poco cuidadoso me parece merecedora de reproche, pero en sede administrativa o, incluso, extrajudicial. No olvidemos la posibilidad de los propios Colegios de Médicos de amonestar a sus miembros, y que están en disposición de hacerlo en estos casos amparándose en el artículo 27.7 del Código de Ética y Deontología Médica de 1978 (actualizado en 2011), que especifica el deber del médico de preservar la confidencialidad de los pacientes.

de los mismos, si estamos a lo dispuesto en la terminología de la rúbrica del capítulo IV del Título XIX) con objeto de tutelar de manera específica la confidencialidad de determinados secretos o informaciones. Al tratarse de un delito especial, el sujeto activo deberá, como ya hemos señalado, ser funcionario público pero, además, deberá tratarse de un funcionario que tenga una custodia –ideal o intelectual– de la información que genere un deber específico de discreción. La conducta que se incrimina es la revelación, es decir, la comunicación a una tercera persona de lo que no debe divulgarse. Se trata de un tipo de participación necesaria, de manera que la consumación exige el conocimiento de la información por parte de un tercero que no esté autorizado. La interpretación de este delito plantea, no obstante, una serie de interrogantes, como cuánto durará el deber de sigilo tras abandonar el funcionario su cargo. Asuntos como la definición de lo que es un secreto o una información de carácter reservado también son objeto de controversia, y la concreción de la pena dependerá de que se haya causado o no un grave daño para la causa pública o para un tercero, y de la afección a secretos de un particular relacionados con informaciones que tengan la consideración de sensibles o relevantes.

Además de lo anterior, un asunto fundamental a analizar es el conflicto de deberes que puede surgir cuando se solicita legalmente al profesional sanitario (sea funcionario o no) aportar información que conoce. En dichos casos, hemos de analizar el caso concreto y valorar si concurre alguna de las causas de exclusión al secreto profesional.

4. Causas de exclusión del secreto profesional

A pesar de que la base de cualquier sistema sanitario es el respeto a la confidencialidad de todo aquello que el paciente haya confiado al facultativo a lo largo de su relación entre médico y paciente[20], el deber de proteger los secretos profesionales no es absoluto. En algunos supuestos, el profesional sanitario podrá (y, en ocasiones, deberá) revelar información considerada secreta. Y es que, aunque la historia clínica es un instrumento cuyo objetivo es la prestación de la asistencia sanitaria, también puede destinarse a otras finalidades como las judiciales, las de investigación o las de docencia, entre

[20] De Lorenzo y Montero, Ricardo / Escudero González, Marta, "El derecho de acceso a la historia clínica y la seguridad del paciente. Título III. Derecho de las Personas. Artículo 15 (7.6 y 8)", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Dir.), Ed. Aranzadi, España, 2010, pp. 1196-1218.

otras[21]. Hay que recalcar que el acceso del propio facultativo a la información tampoco es absoluto y total: se limita a los pacientes a los que esté asistiendo. Tratamos aquí, por lo tanto, el caso de aquellos profesionales sanitarios que, habiendo tenido acceso a información de sus propios pacientes (y no habiendo llevado a cabo, en consecuencia, ningún acceso indebido) actúan sin garantizar debidamente el secreto profesional.

Pues bien: incluso en este supuesto, en el que parece indudable que se han vulnerado los derechos del paciente, existen casos en los que la legislación permite la transmisión de información sin consecuencias en el ámbito penal para el sujeto activo[22].

Y es que, al igual que sucede con la confidencialidad, el valor del secreto profesional en el ámbito sanitario también es instrumental, puesto que solo es defendible cuando contribuye a otros fines deseables. Su protección no puede ser un medio para fines delictivos, siendo obligación del facultativo velar para que la misma no genere daño a terceras personas, no ampare el fraude ni la comisión de ningún delito ni, por último, lesione el orden público. Sus causas de exclusión se reflejan tanto en los códigos deontológicos profesionales como en la legislación, y están orientados, sobre todo, a evitar un posible daño o a garantizar el cumplimiento de un imperativo legal.

4.1. Estado de necesidad

La existencia[23] de bienes jurídicos como el patrimonio genético o la salud general hacen que, en determinadas circunstancias, el médico pueda invocar en el desempeño de su profesión figuras jurídicas como el estado de necesidad. No obstante, para que pueda hacerlo deben cumplirse de manera obligatoria una serie de requisitos recogidos en el artículo 20.5 del propio Código Penal. En primer lugar, el objetivo del facultativo debe ser evitar un mal propio o ajeno (siendo esta su motivación para lesionar el bien jurídico de otra persona o infringir su deber). Además, existen tres requisitos: que

---

[21] Vázquez de Castro, Eduardo, "La historia clínica como fichero de datos personales: responsabilidad por inobservancia de la Ley Orgánica de Protección de Datos Personales en su gestión", *Derecho y salud como realidades interactivas,* Cayón De Las Cuevas, Joaquín (Coord.), Ed. Aranzadi, España, 2015, pp. 125-162.

[22] Santander Cartagena, Fernando / del castillo, Carlos, "El respeto a la confidencialidad en el contexto sanitario", *Revista Norte de Salud Mental,* Núm. 16, Vol. 5, 2003, pp. 18-19. Se específica, que incluso en este caso se deberá revelar la menor información posible, solo la necesaria y suficiente.

[23] De la Cuesta Aguado, Paz M., "Estado de necesidad: estructura normativa y naturaleza jurídica", *Revista Aranzadi de Derecho y Proceso Penal,* Núm. 17, 2007, pp. 93-110.

el mal causado no sea mayor que el que se trate de evitar, que la situación de necesidad no haya sido provocada de manera intencionada, y que quien invoca esta figura no tenga, por su oficio o cargo, obligación de sacrificarse. El objetivo debe ser evitar un daño propio o ajeno.

En el primer caso, cuando el fin sea evitar un riesgo vital grave, como unas lesiones severas o la muerte; en el segundo, cuando el profesional sanitario tenga una sospecha fundada de un perjuicio cierto y severo a terceras personas concretas (en ningún caso a terceros en sentido abstracto). Podría utilizarse en casos en los que existe un elevado riesgo de transmisión de una enfermedad a un tercero por parte del propio paciente, cuando la misma no sea una de las llamadas Enfermedades de Declaración Obligatoria (puesto que, cuando nos referimos a las mismas, la figura adecuada a invocar por el facultativo es la del cumplimiento de un deber, al existir una obligación de informar al centro de salud pública que corresponda para proteger a la comunidad).

4.2. Cumplimiento de un deber

El artículo 20.7 del Código Penal hace referencia a quienes llevan a cabo sus acciones obrando en cumplimiento de un deber o en el ejercicio legítimo de un derecho, oficio o cargo. El médico, por las características de su profesión, puede tener acceso a hechos o datos cuyo conocimiento, si bien debería estar amparada por el deber de secreto profesional, colisiona con la persecución de los hechos tipificados como delito en la legislación penal[24]. Atendiendo al artículo 262 del Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal (LECrim), los profesionales de este sector no pueden ampararse en el derecho al secreto médico para no denunciar los hechos delictivos de los que puedan tener conocimiento en el ejercicio de su profesión. De hecho, refuerza esta obligación de manera expresa para los Profesores de Medicina, Cirugía o Farmacia. Del mismo modo, existe también no un derecho, sino un deber de comparecer y declarar como testigos siempre que sean requeridos para ello por las autoridades encargadas de la investigación criminal (en estos casos, la declaración quedará limitada a lo estrictamente necesario y relevante para el objetivo de la investigación judicial, estando la misma basada en la defensa del interés público).

Además, existirán ocasiones en las que los facultativos no acudirán por sí mismos a poner en conocimiento de la autoridad correspondiente unos

[24] López López, Alberto Manuel, "Incorporación al proceso penal de datos relativos a la salud de las personas", *Actualidad jurídica Aranzadi,* Núm. 625, 2004, pp. 2-6.

hechos delictivos, sino que lo harán en respuesta a un requerimiento de la propia Administración de Justicia. De nuevo, el deber de guardar secreto del médico no le exime[25] de la obligación de colaborar en este sentido. El profesional sanitario puede encontrarse ante dos escenarios: si la petición cuenta con el consentimiento o autorización del propio paciente a la revelación de la información solicitada por terceros, como es lógico, no existirá ningún obstáculo legal para el cumplimiento al requerimiento judicial, pudiendo entregar la información al Juez. En cambio, en ausencia de este consentimiento o autorización (por ejemplo, por haber solicitado la información una parte distinta al paciente), corresponderá exclusivamente al Juez, y en ningún caso al facultativo, valorar la pertinencia, utilidad y proporcionalidad de la información interesada, debiendo trasladar esta argumentación a la petición de manera que el facultativo, al recibirla, pueda verificar que se han valorado y tenido en cuenta estos criterios. Debe tratarse de una información concreta que interese al proceso, y no una petición general de información. De no cumplirse los requisitos mencionados, el facultativo deberá, sin desacatar el requerimiento judicial efectuado, solicitar al Tribunal que los cumpla. En último lugar, procederá a guardar toda la información en la historia clínica.

Por último, debemos encuadrar aquí la comunicación de casos de enfermedades infectocontagiosas (las ya mencionadas Enfermedades de Declaración Obligatoria), debiendo ceñirse el médico siempre de manera estricta a informar en relación con aquellas enfermedades que se encuentren calificadas como tal, y no a enfermedades en general.

5. Análisis jurisprudencial

La propia doctrina[26] sostiene que las condenas por violación del secreto profesional recaídas sobre profesionales sanitarios son muy pocas en la jurisprudencia española.

---

[25] Izquierdo Blanco, Pablo / Picó i Junoy, Joan (Dirs.), *et ál.*, *La protección del consumidor por mala práxis médica, en centros de salud, psiquiátricos y geriátricos. Aspectos civiles, penales, administrativos y* procesales, Ed. Bosch, Barcelona, España, 2018, pp. 65-66. En opinión de los autores, lo que justifica el quebrantamiento del deber de guardar secreto no es la petición en sí misma, sino la argumentación judicial sobre la necesidad de la información. En consecuencia, la valoración de la utilidad, pertinencia y proporcionalidad de la información por parte del Juez será un requisito indispensable.

[26] Tomás-Valiente Lanuza, Carmen, "Capítulo I. Del descubrimiento y revelación de secretos", *Comentarios prácticos al Código Penal. Tomo II*, Gómez Tomillo, Manuel (Dir.), Ed. Thomson-Reuters-Aranzadi, Cizur Menor, 2015, pp. 653-698.

En nuestro análisis de la misma, encontraremos muchas de las figuras expuestas en los apartados anteriores, dentro de las cuales los Tribunales han encuadrado lo sucedido en la realidad matizando algunos de los elementos teóricos. En la Sentencia 574/2001, de 4 de abril, de la Sala de lo Penal del Tribunal Supremo, encontramos un ejemplo de la aplicación del artículo 199.2 del Código Penal. En ella, se condena a una neuróloga que, tras tener acceso de manera legítima a la historia clínica de una paciente a la que reconoció por ser ambas de la misma pequeña localidad, revela que la misma había abortado en dos ocasiones. Hay que destacar que la persona a la que reveló la información fue su propia madre, que después se lo comunicó a la hermana de la paciente. De aquí puede deducirse que el profesional no está exento del deber de secreto ni siquiera cuando se relaciona con sus parientes más cercanos o sus seres queridos. Se específica, además, que para que la conducta encaje en el tipo delictivo basta con comunicar el secreto por cualquier medio, aunque no sea a una pluralidad de personas, toda vez que la lesión al bien jurídico protegido (la intimidad) se produce independientemente del número de personas que tenga conocimiento de la información que no debió haber sido compartida. Además, el Tribunal entra a distinguir entre la conducta típica de la mera indiscreción: la clave estará en que lo comunicado afecte a la esfera de la intimidad que el titular quiere defender. En el caso mencionado, se considera que el hecho comunicado alcanza la relevancia jurídica suficiente al lesionar la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás que es necesario, de acuerdo a las pautas de nuestra cultura, para mantener una calidad mínima de vida humana.

El Auto 498/2003, de 18 de junio, de la Sección 23ª de la Audiencia Provincial de Madrid introduce un matiz interesante, al determinar que no queda dentro del ámbito de protección de este artículo transmitir cierto tipo de informaciones. Poner en conocimiento de un juzgado un hecho consistente en un ingreso hospitalario y en la identidad de las personas o facultativos que atendieron al paciente no es equiparable a revelar el contenido de una historia clínica o un dato esencial perteneciente a la misma. Al no aportarse ningún dato sobre la dolencia efectiva de la que fue tratado, el tratamiento recibido o su evolución, se manifiestan serias dudas, desde un punto de vista objetivo, de que lo revelado pueda ser considerado un secreto. Éste fue uno de los criterios utilizados para confirmar el auto de sobreseimiento provisional que no condenó por los hechos enjuiciados a sus autores.

En este caso, considero que la decisión fue la correcta y, no obstante, cabe preguntarse si poner en conocimiento de terceras personas los ingresos

hospitalarios y la identidad de los facultativos que atienden al paciente sin dar ningún otro dato más no podría ser, bajo determinadas circunstancias, constitutivo de delito. Sirva como ejemplo la información sobre reiterados ingresos de una persona específicamente en la planta de psiquiatría de un determinado hospital, con objeto de ser atendida por psiquiatras. Aunque, en efecto, no se aporta ningún dato contenido en la historia clínica, creo que esta información ya es, de por sí, suficiente para afectar a la intimidad del paciente. Con objeto de garantizar los derechos de su paciente y de protegerse legalmente, el profesional que transmita esta clase de información deberá, en mi opinión, ser cauteloso y no considerar que toda información que queda fuera de la historia clínica es transmisible a terceros.

La Sentencia 778/2013, de 22 de octubre, de la Sección 1ª de la Sala de lo Penal del Tribunal Supremo sirve para ilustrar lo expuesto en el análisis teórico: se desestima que el acusado haya incurrido en el tipo delictivo del artículo 199.2 del Código Penal cuando queda demostrado que no realizó la acción típica de divulgar a terceros secretos con incumplimiento del deber de sigilo a que está obligado, ya que se limitó a denunciar unos hechos de los que tuvo conocimiento por su actividad profesional, cumpliendo así la obligación legal del artículo 262 de la Ley de Enjuiciamiento Criminal. Es más: al entender que unos determinados hechos podían ser constitutivos de delito, el profesional sanitario se asesoró para poder cumplir con su obligación de manera correcta antes de actuar. De nuevo, la prudencia aparece como fundamental para el facultativo que quiera poner en conocimiento de las autoridades hechos constitutivos de delito. El asesoramiento previo a la comunicación de la información es un elemento a destacar en este caso en concreto, pero es altamente recomendable a nivel general para evitar problemas posteriores.

En efecto, la cuestión de si el facultativo puede transmitir la información contenida en historias clínicas de pacientes que no esté tratando él, sino otro profesional sanitario del mismo centro donde trabaja, sobre todo si la causa parece legítima y pretende poner en conocimiento de las autoridades un delito, resulta de enorme interés. La propia Sentencia 778/2013 nos da la respuesta al explicar que el acusado detectó una serie de irregularidades y, tras asesorarse, con la intención de realizar averiguaciones y transmitir la información que pudiese probar la existencia de delito, se hizo tanto con historias clínicas como con historiales de clientes (documentos internos que contenían información como la contratación de servicios médicos o los importes facturados).

En relación con sus propios pacientes, el Tribunal consideró que, a pesar de haber sido asesorado y haber recibido el apoyo del Ministerio Fiscal, la absolución de este delito no debía basarse en un error de prohibición invencible, sino por estar justificada su conducta al amparo del artículo 20.7 del Código Penal, al estar cumpliendo un deber. Por lo tanto, consideró el Tribunal que el acusado no realizó la acción típica de divulgar a terceros secretos incumpliendo el deber de sigilo al que estaba obligado, sino que cumplió con la obligación legal de denunciar unos hechos de los que tuvo conocimiento por su actividad profesional, que entendió eran constitutivos de delito, y todo esto tras asesorarse sobre su obligación y la manera en que debía actuar. Ahora bien: no sucedió lo mismo con aquellas personas que no eran sus pacientes. En relación con la información concerniente a dichas personas, el Tribunal sí consideró el acceso ilícito y subsumible en el artículo 197 del Código Penal, no permitiendo que ni el acceso ni la revelación posterior se escudasen en la causa de justificación. Pese a todo, el Tribunal sí apreció el error de prohibición invencible y acabó absolviendo al facultativo.

¿Qué sucede cuando la información se revela a nivel interno, dentro del ámbito de instituciones pertenecientes al sistema sanitario, o relacionadas con el mismo? En la Sentencia 90456/2014, de 5 de diciembre, de la Sección 2ª de la Audiencia Provincial de Vizcaya, los compañeros de un facultativo creyeron apreciar en él síntomas de una enfermedad mental, motivo por el cual remitieron al Colegio de Médicos de Vizcaya y a la Dirección de gerencia del Hospital de Galdácano un escrito acompañado de documentación con información sensible. En primer lugar, es importante la manera en la que la Audiencia valoró el hecho de que unos médicos divulgasen información de un compañero también médico: remitiéndose al Código de Ética y Deontología Médica, resaltó la obligación de denunciar las deficiencias que se aprecien en el sistema sanitario y de velar para que en él se den los requisitos de calidad, suficiencia asistencial y mantenimiento de los principios éticos. La cuestión fundamental es, por lo tanto, si el hecho de haber revelado la información en un ámbito tan específico afecta a que la conducta pueda encajar o no en el artículo 199.2. En relación con este particular, la Audiencia afirmó que se trata de un delito en el que el elemento subjetivo del injusto debe abarcar todos los elementos del tipo dada su naturaleza dolosa, y el sujeto activo debe conocer y querer que la divulgación se realice fuera del ámbito de colaboración profesional. Así, no se cumpliría el tipo cuando el *dolo* no abarca la difusión fuera del mismo, o cuando permanece dentro y se persiguen finalidades inherentes al ámbito profesional en el que se han generado. Por lo tanto, al no haberse difundido o divulgado por los acusados la información a nadie además de al Colegio Oficial de Médicos

de Vizcaya y a la Dirección de gerencia del Hospital de Galdácano en el que trabajaban tanto ellos como el denunciante, la conducta no encajaba con la del artículo 199.2 del Código Penal. No se consideró a ninguno de los dos destinatarios públicos de la información, sino que se entendió que ambos estaban legitimados para conocerla y actuar de acuerdo a sus competencias por estar relacionada con un conflicto laboral derivado de la existencia de una posible patología psiquiátrica subyacente. Esto, con independencia de que, como ocurrió, la información se difundiese posteriormente a terceros: al no poder demostrarse que los acusados participaron en dicha difusión, tampoco se les condenó por ello.

Y es que la jurisprudencia insiste en que no basta con la divulgación de la información, sino que es necesario poder atribuírsela a una persona en concreto. Es lo que exige la Sentencia 193/2018, de 13 de marzo, de la Sección 16ª de la Audiencia Provincial de Madrid, que evidencia que demostrar que el sujeto activo incurrió en la conducta típica puede revestir una especial dificultad cuando nos referimos al artículo 199.2. En la misma, se acusó a dos enfermeras del Centro de Salud Parque Coimbra de Móstoles, en Madrid, de acceder a la historia clínica de una de sus compañeras de trabajo del área administrativa que, además, también era paciente del citado centro. En la huella informática de la historia clínica de la denunciante constaban varios accesos por parte de estas enfermeras, pero se consideró que no había quedado suficientemente probado que fueran ellas las que revelaron o comunicaron datos obtenidos de la misma. La Audiencia valoró el clima laboral profundamente deteriorado existente en el centro y la mala relación laboral y personal entre la denunciante y las denunciadas, pero también tuvo en cuenta que la primera nunca oyó a las acusadas dirigirse a ella en términos que evidenciasen que habían tenido acceso a la historia clínica, ni tampoco sabía si a través de ellas terceras personas tuvieron conocimiento de su contenido. Resultó ser cierto que en el centro de salud se conocía un problema médico de la denunciante, pero se consideró que esto no significaba, por sí mismo, que las acusadas fuesen quienes habían difundido la información, puesto que la noticia de hechos de estas características podía haberse propagado por otras vías.

Además, se mencionó el hecho de que antes del deterioro de las relaciones de la denunciante con sus compañeras ésta hizo confidencias muy íntimas a terceras personas que testificaron en el juicio, de manera que la fuente de la manera en la que la información se había extendido por el centro era, como mínimo, dudosa. Ninguna de las demás trabajadoras del centro, incluyendo a aquellas que eran favorables a la denunciante, pudo dar testimonio de

haber oído a las acusadas hacer comentarios con información contenida en la historia clínica. El resultado fue la absolución, toda vez que no se acreditó en absoluto que datos personales y reservados de la denunciante, derivados de su historia clínica, hubieran sido revelados por parte de las acusadas.

No obstante, y pese a la absolución, pueden encontrarse más detalles de interés en esta sentencia, dado que la Audiencia trató de delimitar el tipo penal al que hubiese acudido en caso de haber probado que las acusadas fueron quienes revelaron los secretos. De haber tenido lugar un acceso ilícito, el artículo 197.2 hubiese sido el adecuado para encuadrar esta conducta, quedando el 197.3 reservado para cuando, como sucede en este caso, haya una revelación de la información. Por el contrario, cuando el acceso pueda considerarse lícito (un médico que entra en la historia clínica de su propio paciente), estaríamos ante un hecho atípico, habiendo delito solo si a esto se añade la revelación de la información. En consecuencia, la Audiencia consideró que, de haber tenido lugar el acceso por parte de las acusadas, hubiese sido lícito. La posibilidad de sancionar la hubiese dado el artículo 199, pero solo si se hubiese podido probar la revelación posterior de la información.

6. Conclusiones

El secreto médico es uno de los pilares en los que se fundamenta la relación entre médico y paciente. La seriedad y responsabilidad que debe regir la actividad profesional del propio facultativo y el principio de subsidiariedad, que determina que el derecho penal debe ser la *ultima ratio*, deberían hacer innecesaria la utilización del Código Penal en este ámbito. El Código de Ética y Deontología Médica de 1978 protege la confidencialidad en varios de sus artículos, consagrando de manera específica en su artículo 27.7 el deber del médico de preservar en su ámbito social, laboral y familiar la confidencialidad de los pacientes. A su vez, los Colegios de Médicos tienen la potestad de amonestar a sus miembros. Es lo que sucede, por ejemplo, en el Ilustre Colegio Oficial de Médicos de Madrid, cuyos Estatutos determinan en su artículo 63.3.b como falta disciplinaria muy grave la violación dolosa del secreto profesional. El artículo 64 del mismo texto, en su apartado 4, sanciona esta clase de faltas con suspensión del ejercicio profesional por tiempo superior a un año e inferior a dos y, en caso de reiteración de las mismas, con la expulsión de la Corporación Colegial.

Además, su apartado 5 sostiene que la expulsión del Colegio lleva anexa la inhabilitación para incorporarse a cualquier otro salvo que sea autorizado

de manera expresa por el Consejo General. Si bien es una sanción que solo puede imponerse por la reiteración de faltas muy graves y mediando acuerdo adoptado por la mayoría del Pleno de la Junta Directiva, evidencia la posibilidad para el paciente que ha visto vulnerados sus derechos de presentar su caso ante la Corporación Colegial con importantes consecuencias para el facultativo, quien podría no solo verse suspendido del ejercicio profesional sino, en los casos más graves, expulsado de la misma e inhabilitado para incorporarse a cualquier otra. Por lo tanto, una primera línea de defensa para el paciente que ha visto divulgada la información contenida en su historia clínica es la que establecen los propios Colegios de Médicos. No obstante, en ocasiones, será muy difícil poder demostrar que el facultativo ha accedido indebidamente a la historia clínica o que, siendo correcto el acceso a la misma, se ha divulgado su contenido por parte del profesional sanitario obligado al secreto. En estos casos, quien ha visto lesionado su derecho debe interponer una denuncia amparándose, dependiendo del caso, en alguno de los artículos analizados del Código Penal. Con las pruebas que pueda aportar, o con la investigación del Ministerio Fiscal, se pondrían en marcha los mecanismos del derecho penal.

Y es que la posible incidencia del corporativismo (que existe en el sector sanitario del mismo modo que está presente en muchos otros) o de la influencia y poder del sujeto activo hace necesario, en ocasiones, acudir a un terreno imparcial donde se equilibren las posiciones. Atendiendo a la importancia del bien jurídico protegido, es adecuado que el Estado utilice todos los medios técnicos y humanos a su disposición para saber si se ha visto lesionado, defendiendo así los intereses del paciente. Atendiendo a la jurisprudencia, resulta fundamental, para poder defenderlos, la cuidadosa delimitación de quién puede tener acceso a la historia clínica, y las obligaciones que conlleva esta autorización.

Los artículos 197 y siguientes encuadran una gran variedad de conductas: el acceso sin autorización a la historia clínica (artículo 197.2), su modificación[27] (197.2) y, también, la difusión de su contenido (197.3). Los facultativos no pueden acceder a historias clínicas no autorizadas, de manera que en el caso del artículo 197.3, párrafo primero, en relación con el artículo 197.2, lo que se persigue es la difusión, revelación o cesión de datos derivados de accesos no autorizados, por mucho que el médico tenga permiso para

[27] La Sentencia del Tribunal Supremo 798/2017, de 11 de diciembre de 2017, expone en sus hechos probados la manera en que se procedía a añadir un falso dictamen médico psiquiátrico que justificase la práctica del aborto, asegurando la existencia de grave peligro para la salud psíquica de la madre.

acceder al sistema general con objeto de acceder a las historias clínicas de sus propios pacientes. Habiendo divulgación de la información, acudir al artículo 197 y siguientes o al 199.2 dependerá de si el sujeto activo es un facultativo con autorización para acceder a la historia clínica o no, y de si el acceso ha sido autorizado. Una crítica que podría hacerse en este sentido es que, por mucho que tuviese permiso para acceder a la historia clínica, la misma conducta realizada por un facultativo debería tener un mayor desvalor de la acción al estar obligado al secreto profesional. Y es que el artículo 197.3, párrafo primero, en relación con el artículo 197.2 castiga esta conducta con pena de prisión de dos a cinco años, mientras que el artículo 199.2 prevé una pena de uno a cuatro años.

El artículo 199.2, por su parte, es una herramienta adecuada para encuadrar la conducta del facultativo que divulga aquellos secretos que, por razón de su profesión, debería guardar. Es necesario realizar una matización en este punto: no se trataría de los datos a los que hubiese tenido acceso de manera indebida, como la historia clínica de un paciente al que no está atendiendo, sino de los datos a los que hubiese accedido de manera legítima, pero en relación con los cuales no haya mantenido su obligación de guardar el secreto profesional, como la historia clínica de sus propios pacientes. Al ser la pena prevista de uno a cuatro años de prisión el juzgador podrá valorar si se trata de un caso que haya lesionado gravemente el bien jurídico protegido y merezca una pena de prisión o, por el contrario, se trata de comentarios poco susceptibles de lesionarlo que merecen un reproche menor. En este sentido, y sobre todo en un ámbito en el que hay una casuística tan variada, soy partidario de dotar al juzgador de herramientas jurídicas que le permitan recorrer una banda punitiva para poder mostrarse severo en los casos donde se produzca una profunda lesión al bien jurídico protegido, pero, al mismo tiempo, le hagan posible terminar el proceso con una condena casi simbólica en aquellos casos de escasa gravedad que así lo merezcan.

No obstante, lo más importante es que la actual legislación protege de manera adecuada tanto la intimidad como los datos de carácter personal reservados. Y pese a todo, hay que tener en cuenta que el paciente no sabe cuándo ha tenido lugar un acceso indebido a su historia clínica, de manera que una medida garantista sería un sistema automático de alerta que informase al encargado de proteger dichos datos del acceso no autorizado, obligándole a poner en conocimiento de la persona afectada lo sucedido para que pueda decidir, por sí misma, si existe alguna explicación y, por lo tanto, no desea llevar a cabo acción alguna, si ponerlo en conocimiento del Colegio de Médicos que corresponda o si, directamente, desea trasladar lo sucedido

a las autoridades competentes mediante la interposición de una denuncia. En la actualidad, no existe un sistema de estas características, por lo que muchos accesos indebidos y posteriores filtraciones de información quedan, a buen seguro, sin investigar. El problema no radicaría tanto en el articulado del Código Penal, sino en las dificultades del sujeto pasivo para tener noticia de que sus derechos han podido ser vulnerados. Nos encontramos, por lo tanto, no ante un problema sustantivo, sino de prueba.

Como conclusión, sintetizando el análisis realizado, considero que la manera de proteger a los pacientes en este ámbito debe basarse en tres pilares.

Primero, la mejora en el sistema de detección de accesos indebidos a la historia clínica, de manera que los encargados de custodiar los datos tengan conocimiento de esta clase de accesos de manera automática, estando obligados a ponerlos en conocimiento del paciente afectado, con independencia de que la información contenida en el mismo se divulgue. Solo así puede evitarse que el paciente se entere por terceras personas de que se ha producido dicha infracción, evitándole las dificultades inherentes a este conocimiento tardío, como la posibilidad de que el delito haya prescrito por el paso del tiempo.

Segundo, la necesidad de educar a los profesionales sanitarios también en el ámbito de la protección de datos. En efecto, del mismo modo en que llegó un punto en que se consideró que la transmisión de principios bioéticos era imprescindible en la formación de los médicos, también se ha llegado al momento histórico en que los juristas deben transmitir, de forma clara, comprensible y sencilla, los derechos que amparan a los pacientes en este sentido. Esto tiene un doble objetivo ya que, por un lado, se refuerza la protección a los propios pacientes, pero, además, se garantiza que la amplísima mayoría de facultativos que actúan de buena fe eviten incurrir en errores involuntarios, protegiéndoles también a ellos y evitando que sufran los perjuicios de un proceso penal.

Tercero, la posibilidad de una reforma localizada en la estructura de los artículos 197 a 201 del Código Penal español, orientada a tener en cuenta detalles como el mayor desvalor de la acción cuando el facultativo divulga la información contenida en una historia clínica a la que ha accedido de manera lícita, por haberse depositado en él la confianza suficiente para darle acceso al sistema en el que se albergan las historias clínicas. A pesar de esta propuesta orientada únicamente a mejorar el nivel de protección de los pacientes, la actual redacción de estos artículos no acusa, a mi juicio, problemas graves

que requieran una atención inmediata por parte del legislador. No obstante, considero que modificaciones puntuales como la propuesta podrían ser positivas siempre que al tiempo que se protegen los derechos de los pacientes se tenga también en cuenta que debemos evitar, siempre que sea posible, la imposición de penas de prisión o de inhabilitación a los miembros de una profesión como es la sanitaria, quienes solo pretenden realizar una excelente y loable labor que busca beneficiar y proteger a los pacientes tanto como los juristas deseamos protegerlos mediante la regulación del ordenamiento jurídico.

7. Bibliografía

Caruso Fontán, María Viviana, "La responsabilidad penal de los encargados de bases de datos de ADN frente a la cesión de información contenida en los registros", *Revista de Derecho Penal,* Núm. 40, 2003.

De la Cuesta Aguado, Paz M., "Estado de necesidad: estructura normativa y naturaleza jurídica", *Revista Aranzadi de Derecho y Proceso Penal,* Núm. 17, 2007.

De la Mata Barranco, Norberto Javier, *Derecho Penal europeo y legislación española: las reformas del Código Penal,* Ed. Tirant lo Blanch, Valencia, España, 2015.

De la Mata Barranco, Norberto Javier, "El funcionario público ante el Derecho Penal", *Revista jurídica de Castilla y León,* Núm. 20, 2010.

De Lorenzo y Montero, Ricardo / Escudero González, Marta, "El derecho de acceso a la historia clínica y la seguridad del paciente. Título III. Derecho de las Personas. Artículo 15 (7.6 y 8)", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Dir.), Ed. Aranzadi, España, 2010.

Dopazo Fraguío, Pilar, "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (novedades del Reglamento General de Protección de Datos)", *Revista española de derecho europeo,* Núm. 68, 2018.

Escuchuri Aisa, Estrella, "Comisión de delitos en el marco de organizaciones y grupos criminales. Algunos problemas que plantea la regulación del Código penal español en relación con la delincuencia organizada", *Revista Aranzadi de Derecho y Proceso Penal,* Núm. 37, 2015.

Fernández Pantoja, Pilar, "El delito de revelación y divulgación de secretos en el ámbito sanitario", *Estudios jurídicos sobre responsabilidad penal, civil y administrativa del médico y otros agentes sanitarios,* Ed. Dykinson, Madrid, España, 2010.

García Albero, Ramón, *Comentarios al Código Penal (Tomo II),* Ed. Aranzadi, Cizur Menor, España, 2008.

Izquierdo Blanco, Pablo / Picó i Junoy, Joan (Dirs.), *et ál*, *La protección del consumidor por mala práxis médica, en centros de salud, psiquiátricos y geriátricos. Aspectos civiles, penales, administrativos y* procesales, Ed. Bosch, Barcelona, España, 2018.

López López, Alberto Manuel, "Incorporación al proceso penal de datos relativos a la salud de las personas", *Actualidad jurídica Aranzadi,* Núm. 625, 2004.

Morales Prats, Fermín, "Reflexiones político criminales sobre los límites de la intervención penal en los delitos contra la privacy (sic): la reforma del CP de 2015 (LO 1/2015)", *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo,* Bacigalupo, Silvina / Feijoo Sánchez, Bernardo José / Echano Basaldúa, Juan Ignacio (Coords.), Ed. Universitaria Ramón Areces, España, 2016.

Nicolás Jiménez, Pilar, "La protección de los datos genéticos de carácter personal en Derecho Penal español: un caso práctico", *Temas de Derecho penal: libro homenaje a Luis Guillermo Cornejo Cuadros,* Armaza Armaza, Emilio José / Mendoza Valdez, José / De Miguel Beriain, Iñigo / Urruela Mora, Asier (Coords.), Ed. Adrus, Arequipa, Perú, 2008.

Obispo Triana, Concepción, "Circular 3/2017, de 21 de septiembre, sobre la reforma del código penal operada por la LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos", *Revista Aranzadi Doctrinal,* Núm. 10, 2017.

Romeo Casabona, Carlos María, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", *Derecho Penal, Parte Especial*, Romeo Casabona, Carlos María / Sola Reche, Esteban / Boldova Pasamar, Miguel Ángel (Coords.), Ed. Comares, España, 2016.

Romeo Casabona, Carlos María, *Los delitos de descubrimiento y revelación de secretos: especial consideración a su comisión en conexión con las nuevas tecnologías de la información y de la comunicación,* Ed. Tirant lo Blanch, Valencia, España, 2005.

Romeo Casabona, Carlos María, *Comentarios al Código Penal, Parte Especial, Volumen II,* Díez Ripollés, José Luís / Romeo Casabona, Carlos María *et ál* (Coords.), Ed. Tirant lo Blanch, Valencia, España, 2004.

Romeo Casabona, Carlos María, *Las transformaciones del Derecho Penal en un mundo en cambio (Volumen I),* Ed. Adrus, Arequipa, Perú, 2004.

Rueda Martín, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Ed. Atelier, Barcelona, España, 2018.

Santander Cartagena, Fernando / Del Castillo, Carlos, "El respeto a la confidencialidad en el contexto sanitario", *Revista Norte de Salud Mental,* Núm. 16, Vol. 5, 2003.

Suárez-mira rodríguez, Carlos / Judel Prieto, Ángel / Piñol Rodríguez, José Ramón, *Manual de Derecho Penal. Parte Especial,* Ed. Aranzadi, Cizur Menor, España, 2011.

Tomás-Valiente Lanuza, Carmen, "Capítulo I. Del descubrimiento y revelación de secretos", *Comentarios prácticos al Código Penal. Tomo II*, Gómez Tomillo, Manuel (Dir.), Ed. Thomson-Reuters-Aranzadi, Cizur Menor, España, 2015.

Vázquez De Castro, Eduardo, "La historia clínica como fichero de datos personales: responsabilidad por inobservancia de la Ley Orgánica de Protección de Datos Personales en su gestión", *Derecho y salud como realidades interactivas,* Cayón De Las Cuevas, Joaquín (Coord.), Ed. Aranzadi, España, 2015.

DOCUMENTOS / DOCUMENTS

Informe 073667/2018 de la Agencia Española de Protección de Datos sobre la incidencia en el ámbito de la investigación biomédica del Reglamento General de Protección de Datos*

Se solicita que por este Gabinete Jurídico se emita informe acerca de la incidencia que en el ámbito de la investigación biomédica pudiera producir la plena aplicación a partir del 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de 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), así como la aprobación de una nueva Ley Orgánica de Protección de Datos, teniendo en cuenta el texto del Proyecto que fue remitido a las Cortes Generales por el Gobierno el día 10 de noviembre de 2017. Todo ello a la vista de la preocupación manifestada en diversos foros por las sociedades científicas.

Como punto de partida, tratándose de datos relacionados con la salud del interesado, el artículo 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo aprobado por el Real Decreto 1726/2007, de 21 de diciembre, dispone que "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente"

* Informe disponible para su consulta en la página web de la Agencia Española de Protección de Datos: https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

Al propio tiempo debe tenerse en cuenta que, en el momento presente, la materia se encuentra regulada en nuestro país por la Ley 14/2007, de 3 julio, de Investigación Biomédica, que parte en sus artículos 4 y 5 del respeto a los principios de consentimiento del sujeto fuente y protección de sus datos personales.

Estos principios aparecen claramente plasmados en el artículo 5 de la Ley, según el cual:

> "1. Se garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales que resulten de la actividad de investigación biomédica, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las mismas garantías serán de aplicación a las muestras biológicas que sean fuente de información de carácter personal.
> 2. La cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado.
> En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados.
> 3. Se prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento.
> 4. Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación.
> 5. Si no fuera posible publicar los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento previo y expreso de aquélla".

Por otra parte, en lo que respecta a la utilización de muestras biológicas humanas con fines de investigación biomédica, el artículo 58.1 de la Ley parte del principio del consentimiento del sujeto fuente, al establecer que "la obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud. Dicho consentimiento será revocable".

Por su parte, en cuanto a posibles usos secundarios de las muestras obtenidas del sujeto fuente, el artículo 58.2 de la Ley toma también como

base esencial del tratamiento el consentimiento, que "será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización". Sin embargo, introduce en su párrafo segundo una excepción, dado que "de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de esta Ley", previo dictamen favorable del Comité de Ética de la Investigación correspondiente, que deberá tener en cuenta, como mínimo, los requisitos que el propio precepto cita; es decir:

a) Que se trate de una investigación de interés general.

b) Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para la obtención de las muestras.

c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente.

d) Que no conste una objeción expresa del mismo.

e) Que se garantice la confidencialidad de los datos de carácter personal.

Este precepto se complementa asimismo con el artículo 60 de la Ley, que si bien establece en su apartado 1 una regla limitativa a cerca del tratamiento para investigaciones secundarias, flexibiliza dicho criterio en su apartado 2. Así, se establece que

> "1. El consentimiento sobre la utilización de la muestra biológica se otorgará, bien en el acto de obtención de la muestra, bien con posterioridad, de forma específica para una investigación concreta.
> 2. El consentimiento específico podrá prever el empleo de la muestra para otras líneas de investigación relacionadas con la inicialmente propuesta, incluidas las realizadas por terceros. Si no fuera este el caso, se solicitará al sujeto fuente que otorgue, si lo estima procedente, un nuevo consentimiento".

En definitiva, el modelo establecido en el actualmente vigente en materia de investigación biomédica parte, como regla general del consentimiento del sujeto fuente, que no obstante podrá quedar exceptuado en determinados supuestos, bien por no ser posible la identificación del sujeto por haber sido

anonimizados sus datos conforme al artículo 3 i), previo dictamen favorable del Comité Ético de Investigación, bien cuando se trate de una investigación relacionada con la inicial, al considerarse el fin de dicha investigación compatible con el de aquélla en que se prestó el consentimiento. Fuera de estos casos sería, en términos de la Ley, necesario el consentimiento expreso del afectado (artículo 58.1) para una investigación concreta (artículo 60.1).

Una vez perfilado el marco actualmente vigente, debe analizarse el modo en que el mismo podrá verse afectado por el Reglamento General de Protección de Datos, que conforme a su artículo 99.2, producirá plenos efectos el día 25 de mayo de 2018, tratándose así de una norma directamente aplicable en España que desplazará las previsiones de la Ley Orgánica 15/1999 en cuanto no resulten coherentes con este nuevo marco legal.

Como punto de partida, debe señalarse que en el caso de la investigación biomédica, y particularmente en la llevada a cabo a partir de muestras biológicas procedentes del mismo, nos encontraremos ante el tratamiento de datos relativos a la salud de los sujetos fuente, toda vez que el artículo 4.15 del Reglamento los define como "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, *que revelen información sobre su estado de salud*".

En relación con estos datos, el artículo 9.1 del reglamento General de protección de datos parte del principio general de prohibición del tratamiento, al indicar que "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

No obstante, este principio se exceptúa en los supuestos enumerados en el artículo 9.2, siendo especialmente relevantes a los efectos que aquí interesan las letras a) y j) del precepto, que legitiman este tratamiento cuando "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado" y cuando "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de

la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

A su vez, el artículo 89 del reglamento General de Protección de Datos dispone en sus dos primeros apartados lo siguiente:

> "1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.
> 2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines".

Finalmente, en relación con el principio de limitación de finalidad, el segundo inciso del artículo 5.1 b) del reglamento, siguiendo lo establecido hasta ahora en el artículo 4.2 de la Ley Orgánica 15/1999 dispone que "de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales".

La primera conclusión que puede extraerse de la literalidad de las normas que se han venido reproduciendo es la de que el Reglamento general de Protección de Datos no implica una alteración del marco normativo actualmente vigente en España en relación con el tratamiento de datos en el marco de la investigación biomédica. Dichos datos podrán seguir siendo tratados en los términos establecidos en la Ley 14/2007, a cuya habilitación legal se remitiría el artículo 9.2 j) del Reglamento General de Protección de Datos y que establece las garantías de seudonimización (en la redacción del texto "datos

codificados o reversiblemente disociados") y minimización, delimitando igualmente las reglas de limitación de la finalidad en su artículo 60.2.

La cuestión estriba en el alcance que deba prestarse al consentimiento prestado por el interesado para el uso de sus datos con fines de investigación o para que pueda tener lugar un uso secundario con tales fines de datos asistenciales.

A tal efecto, el artículo 4.11 del reglamento define el consentimiento del interesado como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". De ello se desprende que los requisitos exigidos por la Ley Orgánica 15/1999, es decir, que el consentimiento sea libre, inequívoco, específico e informado son exactamente los mismos que establece el nuevo Reglamento.

El concepto de consentimiento previsto en el Reglamento se reproduce por el artículo 6.1 del Proyecto de Ley Orgánica de Protección de Datos, al indicar que "se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Este precepto se complementa con lo establecido en el artículo 6.2, según el cual "Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas".

Ello implica que en los supuestos en que el tratamiento deba fundarse en el consentimiento, el interesado debería conocer de forma clara e inequívoca las finalidades para las que se procederá a dicho tratamiento.

Esta regla, por tanto únicamente sería aplicable a los supuestos en que el consentimiento deba ser prestado como base legal para el tratamiento y no para aquéllos casos en que la Ley habilite el tratamiento sin dicha base legal, como podría suceder, por ejemplo, en los supuestos establecidos en el artículo 58.2 de la Ley de Investigación Biomédica.

Además será preciso interpretar qué debe entenderse por consentimiento "específico e inequívoco" a los efectos relevantes para este informe; es decir, cuál es el sentido de dichos requisitos del consentimiento teniendo en cuenta lo dispuesto en la normativa vigente en materia de protección de datos así como su aplicabilidad al ámbito del tratamiento de datos con fines de investigación biomédica.

Para ello, es preciso atender a los considerandos del propio Reglamento General de Protección de Datos, que clarifican e interpretan el contenido de su articulado.

Pues bien, como punto de partida, el Reglamento realiza una interpretación sumamente amplia del concepto de investigación científica, puesto que según su considerando 159 "El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública".

En este mismo sentido, el artículo 157 amplia el ámbito de la investigación, teniendo en cuenta la posible recogida de datos procedentes de registros. Así, recuerda que "combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros".

Y en relación con el tratamiento de las categorías especiales de datos, señala expresamente el considerando 52 que "deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular (…) con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos" y añade el primer inciso del considerando 53 que "las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto", haciendo nuevamente referencia al tratamiento de los datos con fines de investigación científica.

Finalmente, y de forma totalmente explícita, el considerando 33 del reglamento se refiere, precisamente al consentimiento prestado para el tratamiento de los datos con fines de investigación científica, teniendo precisamente en cuenta el carácter intrínsecamente dinámico de dicha investigación. Así, señala que "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida".

De todo ello se derivaría que los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento no deben ser interpretados en el ámbito de la investigación científica de un modo restrictivo, limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futro ese consentimiento, sin que ello lo vicie en modo alguno, incluso a "finalidades" o áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó sin que sea necesario recabar un nuevo consentimiento del sujeto fuente, teniendo en cuenta los beneficios para los individuos y la sociedad en su conjunto que pueden derivarse de tal investigación no prevista.

De este modo, por poner un ejemplo, no sería preciso, para garantizar el carácter inequívoco y específico del consentimiento, que el mismo fuese prestado para la realización de una investigación concreta; ni siquiera para la realización de investigaciones en una rama muy delimitada, como por ejemplo, un determinado tipo de cáncer, sino que, teniendo en cuenta la interpretación derivada directamente del propio Reglamento, será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, como por ejemplo, la investigación oncológica, o incluso para ámbitos más extensos.

Por todo ello, y completando la conclusión a la que se hacía referencia en el apartado III de este informe, el Reglamento General de Protección de Datos y el Proyecto de Ley Orgánica de Protección de Datos, no sólo mantienen inalterado el régimen contenido en la normativa reguladora de la investigación biomédica, sino que permiten realizar una interpretación más flexible del alcance que puede darse al consentimiento prestado de conformidad con la misma, superando, a título de ejemplo, la interpretación más restrictiva contenida en el artículo 60 de la Ley de Investigación Biomédica.

Al propio tiempo, la interpretación no restrictiva que se ha analizado debería ser tenida igualmente en cuenta por los Comités Éticos de Investigación en los supuestos en los que autorizasen el tratamiento de muestras codificadas, sin contar con el consentimiento cuando no fuera posible su obtención, conforme al artículo 58.2 de la Ley 14/2007.

The European Data Protection Board Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)*

Table of contents : 1. Introduction. 2. Legal basis for the processing of personal data in the course of a clinical trial protocol (primary use). 2.1. Processing operations related to reliability and safety purposes. 2.2. Processing operations purely related to research activities. 3. Secondary uses of clinical trial data outside the clinical trial protocol for scientific purposes. 4. Conclusion.

The European Data Protection Board

Having regard to Article 70.1.b of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING OPINION:

---

* The present opinion, adopted on 23 January 2019, is available at The European Data Protection Board website: https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_es

1. Introduction

1. On 8 October 2018, the European Commission (DG SANTE) has submitted to the EDPB a request for consultation under article 70 of the General Data Protection Regulation concerning a document on "Questions and Answers on the interplay between the Clinical Trials Regulation (CTR)[1] and the General Data Protection regulation (GDPR)[2]" (hereafter the "Q&A).

2. While the GDPR ensures the protection of individuals with regard to the processing of personal data and harmonised rules on the free movement of such data; the CTR aims at ensuring a greater level of harmonisation of the rules for conducting clinical trials throughout the EU. Notably, it introduces an authorisation procedure based on a single submission via a single EU portal, an assessment procedure leading to a single decision, rules on the protection of individuals, and informed consent and transparency requirements

3. It must be recalled that the CTR entered into force on 16 June 2014, however, the timing of its application has been put off as it depends on the development of a fully functional EU clinical trials portal and database. After an independent audit, and a period of 6-months starting from a confirmation notice published by the European Commission, the CTR shall finally become applicable. Consequently, the entry into application of this regulation is currently estimated to occur in 2020.

4. In addition to this, it must be noticed that Article 93 of the CTR provides that "Member States shall apply Directive 95/46/EC [now repealed by the GDPR] to the processing of personal data carried out in the Member States pursuant to this Regulation" and that "Regulation (EC) No 45/2001 [repealed by Regulation 2018/1725] shall apply to the processing of personal data carried out by the Commission and the Agency pursuant to this Regulation". The GDPR as well makes express references to the relevant legislation applicable to clinical trials[3]. It follows that both legislations apply simultaneously and that the CTR constitutes a sectoral law containing specific

---

1 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJEU L 158 27/05/2014.

2 2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJEU L 119 04/05/2016.

3 Recital 156 and recital 161 of the GDPR.

provisions relevant from a data protection viewpoint but no derogations to the GDPR.

5. In order to provide guidance for a consistent data protection approach to clinical trials in the EU, the Q&A of the European Commission addresses a number of topics that - with the exception of Question 11 which explains the current situation under the Clinical Trial Directive – will become more relevant when the CTR becomes applicable. Such topics include: the adequate legal basis, informed consent and its withdrawal, information of data subjects, transfers and secondary uses. While the CTR is not yet applicable, the information provided in those FAQ constitutes a good basis for a GDPR compliant clinical trial.

6. The EDPB understands that there is an urgent need for clarification, in particular after the entrance into force of GDPR, and has decided to concentrate its comments of the drafted Q&A on the issue of the appropriate legal basis for the processing of personal data in the context of clinical trials (primary use) and secondary use of clinical trial data for other scientific purposes.

2. Legal basis for the processing of personal data in the course of a clinical trial protocol (primary use)

7. In the context of this Opinion, the EDPB considers that all processing operations related to a specific clinical trial protocol during its whole lifecycle, from the starting of the trial to deletion at the end of the archiving period, shall be understood as primary use of clinical trial data[4]. However, the EDPB considers that not all processing operations relating to such "primary use" of clinical trial data pursue the same purposes and fall within the same legal basis.

8. The overall objective of the CTR is to achieve a harmonised internal market as regards clinical trials and medicinal products for human use, taking as a starting point a high level of protection of health, while setting high

[4] It has to be noted that this broad interpretation of the primary use of data is different from the concept of primary use in Article 29 Working Party Opinion 03/2013 on purpose limitation of 3 April 2013, WP203, p. 21, which states that the very first processing operation, i.e. the collection of data, is primary use and any processing following collection must be considered "further processing".

standards of quality and safety for medicinal products by ensuring that data generated in clinical trials are reliable and robust[5].

9. When discussing the issue of the legal basis for the processing of personal data during the whole lifecycle of a clinical trial, the EDPB considers relevant to distinguish, two main categories of processing activities. In particular, processing operations purely related to research activities must be distinguished from processing operations related to the purposes of protection of health, while setting standards of quality and safety for medicinal products by generating reliable and robust data (reliability and safety related purposes); these two main categories of processing activities fall under different legal bases

2.1. Processing operations related to reliability and safety purposes

10. The EDPB is of the opinion that the processing operations expressly provided by the CTR and by relevant national provisions, and which are related to reliability and safety purposes, can be considered as falling within "legal obligation(s) to which the controller is subject" under Article 6(1)(c) of the GDPR.

11. The Working Party 29[6] has discussed the conditions under which this legal basis may be applicable: the obligation must be imposed by law; the law must fulfil all relevant conditions to make the obligation valid and binding; the law must comply with data protection law, including the requirement of necessity, proportionality and purpose limitation; the legal obligation itself must be sufficiently clear as to the processing of personal data it requires; the controller should not have an undue degree of discretion on how to comply with the legal obligation The EDPB considers that this is notably the case for obligations relating to the performance of safety reporting under Articles 41 to 43 of the CTR, and obligations concerning the archiving of the clinical trial master file (25 years according to Article 58 CTR) and the medical files of subjects (which is to be determined by national law according to the same provision). The same applies to any disclosure of clinical trial data to the national competent authorities in the course of an inspection in accordance with relevant national rules (see Articles 77- 79 CTR).

[5] Recital 82 CTR and Article 3(b) CTR.

[6] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014, WP 217, p. 19.

12. Therefore, the processing of personal data in the context of safety reporting or in the context of an inspection by national competent authority, or the retention of clinical trial data in accordance with archiving obligations set up by the CTR or, as may be the case, relevant national laws, have to be considered as necessary to comply with legal obligations to which the sponsor and/or the investigator are subject to.

13. The corresponding appropriate condition for lawful processing of special categories of data in the context of these obligations shall be Article 9(2)(i): "processing is necessary for reasons of public interest in the area of public health, such as [...] ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or member State law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".

2.2. Processing operations purely related to research activities[7]

14. Processing operations purely related to research activities in the context of a clinical trial cannot, however, be derived from a legal obligation. Depending on the whole circumstances of the trial and the concrete data processing activity, research related activities may either fall under the data subject's explicit consent (Article 6(1)(a) in conjunction with Article 9(2)(a)), or a task carried out in the public interest (Article 6(1)(e)), or the legitimate interests of the controller (Article 6(1)(f)) in conjunction with Article 9(2)(i) or (j) of the GDPR.

Consent - explicit consent

15. As rightly pointed out in Q&A 4, the informed consent foreseen under the CTR must not be confused with the notion of consent as a legal ground for the processing of personal data under the GDPR.

16. Provisions of Chapter V CTR on informed consent, in particular Article 28, respond primarily to core ethical requirements of research projects involving humans deriving from the Helsinki Declaration. The obligation to obtain

[7] Article 29 Working Party Guidelines on consent under Regulation 2016/679 of 10 April 2018, p. 27 states that the notion of scientific research may not be stretched beyond its common meaning and understand that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.

the informed consent of participants in a clinical trial is primarily a measure to ensure the protection of the right to human dignity and the right to integrity of individuals under Article 1 and 3 of the Charter of Fundamental Rights of the EU; it is not conceived as an instrument for data protection compliance.

17. Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit consent is required when the processing of special categories of data, such as health data, are involved (Article 9(2)(a) GDPR). In order to assess whether the individual's explicit consent can be a valid legal basis for the processing of sensitive data in the course of a clinical trial, data controllers should duly take into account the Working Party 29 Guidelines on consent, and check if all the conditions for a valid consent can be met in the specific circumstances of that trial[8].

18. The EDPB considers that data controllers should pay particular attention to the condition of a "freely given" consent. As stated in the Working Party 29 Guidelines on consent, this element implies real choice and control for data subjects. Besides, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller[9].

19. Depending on the circumstances of the clinical trial, situations of imbalance of power between the sponsor/investigator and participants may occur. The CTR expressly addresses these risks and requires the investigator to take into account all relevant circumstances, in particular whether the potential subject belongs to an economically or socially disadvantaged group, or is in a situation of institutional or hierarchical dependency that could inappropriately influence her or his decision to participate[10].

20. However, it must be kept in mind that even though conditions for an informed consent under the CTR are gathered, a clear situation of imbalance of powers between the participant and the sponsor/investigator will imply that the consent is not "freely given" in the meaning of the GDPR. As a matter of example, the EDPB considers that this will be the case when a participant is not in good health conditions, when participants belong to an economically or socially disadvantaged group or in any situation of institutional or hierarchical dependency. Therefore, and as explained in the

---

8 Article 29 Working Party Guidelines on consent under Regulation 2016/679 of 10 April 2018, as endorsed by the EDPB on 25 May 2018.

9 *Idem*, p.6. See also Recital 43 GDPR.

10 Recital 31 CTR.

Guidelines on consent of the Working Party 29, consent will not be the appropriate legal basis in most cases, and other legal bases than consent must be relied upon (see below alternative legal bases).

21. Consequently, the EDPB considers that data controllers should conduct a particularly thorough assessment of the circumstances of the clinical trial before relying on individuals' consent as a legal basis for the processing of personal data for the purposes of the research activities of that trial.

Withdrawal of consent

22. Along the conditions for consent under both texts, the EDPB considers that the withdrawal of the informed consent, under Article 28(3) of the CTR shall not be confused with the withdrawal of consent under the GDPR. Under the former, it is expressly provided that the withdrawal of the informed consent, which shall not affect the activities already carried out and the use of the data obtained based on informed consent before its withdrawal is "[w]ithout prejudice to the Directive 95/46/EC" (now the GDPR).

23. Under the GDPR, if consent is used as the lawful basis for processing, there must be a possibility for individuals to withdraw that consent at any time (Article 7(3)), and there is no exception to this requirement for scientific research[11]. As a general rule, if consent is withdrawn, all data processing operations that were based on consent remain lawful in accordance with the GDPR (Article 7(3)); however, the controller shall stop the processing actions concerned and if there is no other lawful basis justifying the retention for further processing, the data should be deleted by the controller (see Article 17(1)(b) and (3) GDPR).

24. Consequently, the withdrawal of consent, in accordance with Article 7 GDPR, to the processing of personal data for research purposes must be applied taking into account other purposes of processing based on other lawful grounds. In the context of clinical trials, the data subject's consent is limited to the processing operations purely related to research activities. This implies that in case of withdrawal of consent by an individual, all research activities carried out with the clinical trial data relating to that individual shall cease. However, the withdrawal of consent does not affect the processing operations that are based on other lawful grounds, in particular legal obliga-

[11] WP29, Guidelines on consent under Regulation 2016/679, 28 November 2017, WP259.

tions to which the sponsor/investigator are subject such as the ones related to safety purposes (see point 1.1 above).

Task carried out in the public interest or legitimate interest of the controller

25. The EDPB considers that as an alternative to data subject's consent, the lawful grounds of processing provided under Article 6(1)(e) or 6(1)(f) are more appropriate.

26. The processing of personal data by data controllers could be considered as "necessary for the performance of a task carried out in the public interest" pursuant to Article 6(1)(e) GDPR. Article 6(3) GDPR further provides that this basis shall be laid down by Union or Member State law and that the purpose of the processing shall be laid down in that legal basis. The processing of personal data in the context of clinical trials can thus be considered as necessary for the performance of a task carried out in the public interest when the conduct of clinical trials directly falls within the mandate, missions and tasks vested in a public or private body by national law[12].

27. For all other situations where the conduct of clinical trials cannot be considered as necessary for the performance of the public interest tasks vested in the controller by law, the EDPB will consider that the processing of personal data could be "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" following Article 6(1)(f) GDPR.

28. For the processing of special categories of data, the legal basis identified under Article 6 shall be applied only if Article 9 GDPR provides for a specific derogation from the general prohibition to process special categories of data. The EDPB considers that depending on the specific circumstances of a clinical trial, the appropriate Article 9 condition for all processing operations of sensitive data for purely research purposes could either be "reasons of public interest in the area of public health [...] on the basis of Member State

[12] Recital 45 GDPR states that it does not require a specific law for each individual processing (i.e. for each clinical trial). A law as a basis for several processing operations based on the performance of a task carried out in the public interest may be sufficient. See also Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014, WP 217, p. 21-22.

law" (Article 9(2)(i)), or "scientific ... purposes in accordance with Article 89(1) based on Union or Member State law"(Article 9(2)(j)).

3. Secondary uses of clinical trial data outside the clinical trial protocol for scientific purposes

29. The CTR addresses specifically the issue of secondary use in its Article 28(2) with a specific focus on consent. It refers solely to situations where the sponsor may want to process the data of the clinical trial subject "outside the scope of the protocol", but only – and "exclusively" – for scientific purposes. The CTR considers consent for this specific processing purpose should be sought from the data subject or his/her legally designated representative at the time of the request for informed consent for participation in the clinical trial. However, as discussed above with regard to provisions of Chapter V CTR on informed consent, consent foreseen in article 28(2) CTR is not the same consent referred to in the GDPR as one of the legal basis for the processing of personal data, regardless of whether it is or not the legal ground used for the primary processing.

30. Therefore, as the European Commission points out in its Q&A, namely in question 7, if a sponsor or an investigator would like to further use the personal data gathered for any other scientific purposes, other than the ones defined by the clinical trial protocol, it would require another specific legal ground than the one used for the primary purpose. The chosen legal basis may or may not differ from the legal basis of the primary use.

31. However, the EDPB considers that this approach excludes, in all circumstances, the applicability of the so-called presumption of compatibility provided under Article 5(1)(b) GDPR. This Article provides that where data is further processed for archiving purposes in the public interest, scientific, historical research or statistical purposes, these shall a priori not be considered as incompatible with the initial purpose, provided that it occurs in accordance with the provisions of Article 89, which foresees specific adequate safeguards and derogations in these cases. Where that is the case, the controller could be able, under certain conditions, to further process the data without the need for a new legal basis[13]. These conditions, due to their horizontal and complex nature, will require specific attention and guidance from the EDPB in the future. For the time being, the presumption of compatibility, subject to the conditions set forth in Article 89, should not be excluded, in all circumstances,

[13] Recital 50 GDPR.

for the secondary use of clinical trial data outside the clinical trial protocol for other scientific purposes.

32. In any event, even when the presumption of compatibility will find to apply, the scientific research making use of the data outside the protocol of the clinical trial must be conducted in compliance with all other relevant applicable provisions of data protection as stated under Article 28(2) CTR. Therefore, the controller shall not be deemed exempt from the other obligations under data protection law, for example with regard to fairness, lawfulness (i.e. in accordance with applicable EU and national law), necessity and proportionality, as well as data quality.

4. Conclusion

33. To conclude, the EDPB recommends modifying the Q&A when discussing the lawful grounds for processing to distinguish the processing activities related to reliability and safety that can be directly derived from legal obligations of the controller and which fall within the legal basis of Article 6(1)(c) in conjunction with Article 9(1)(i) of GDPR.

34. For all other processing activities, identified in this Opinion as processing operations purely related to research activities, the Q&A should be modified to reflect three alternative legal bases, depending on the whole circumstances attached to a specific clinical trial:

- a task carried out in the public interest under Article 6(1)(e) in conjunction with Article 9(2), (i) or (j) of the GDPR; or

- the legitimate interests of the controller under Article 6(1)(f) in conjunction with Article 9(2) (j) of the GDPR; or

- under specific circumstances, when all conditions are met, data subject's explicit consent under Article 6(1)(a) and 9(2)(a) of the GDPR.

For the European Data Protection Board

The Chair

Andrea Jelinek

BIBLIOGRAFÍA / BIBLIOGRAPHY

Recensiones de libros y revistas*

*Books and journals reviews***

CRISTEA UIVARU, Lucía: *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud*, Ed. Bosch, Barcelona, España, 2018, 360 pp.

Recientemente, desde la prestigiosa y bien posicionada Editorial Bosch, veía la luz este libro de Lucía CRISTEA UIVARU *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud,* que revisa y adapta su tesis doctoral, dirigida por Carmen PARRA RODRÍGUEZ –Profesora de Derecho Internacional y Directora de la Cátedra UNESCO en Paz, Solidaridad y Diálogo Intercultural de la Universidad Abat Oliba CEU–, quien, en esta oportunidad y por vía de Prólogo, la avala. Su autora, Lucía CRISTEA, Doctora en Derecho por dicha Universidad de Barcelona y Profesora de Derecho Administrativo, actualmente ejerce como abogada y es Vocal de la Comisión de Derecho Sanitario del Ilustre Colegio de Abogados de Barcelona compaginando, de forma comprometida, la actividad docente e investigadora con la profesional. Esta dualidad ha enriquecido sumamente su investigación en la medida en que, por una parte, nos ofrece un exhaustivo análisis tanto de los principios que deben inspirar la utilización de los datos (en concreto, los sanitarios) como de la normativa –en el ámbito de la Unión Europea y en el nacional y autonómico– en la que quedan contenidos; y por otra parte, aborda desde una perspectiva eminentemente práctica, dado ese insoslayable perfil de abogada en ejercicio, los diversos problemas y lagunas que pueden plantearse en los litigios que atañen a la protección de la vida sanitaria de las personas.

La oportunidad de esta publicación queda acreditada no sólo por la antedicha finalidad práctica que pretende, sino porque en ella se incorporan

* Para incluir recensiones en esta Sección se remitirá un ejemplar de la publicación correspondiente a la Dirección de la Revista.

** For reviews of books and journals in this Section, a copy of the publication should be sent to the Editor of the Review.

las últimas novedades acaecidas en el Derecho europeo de protección de datos de salud. Considero que, probablemente, la principal característica de este libro es su carácter pionero y su rabiosa actualidad. No en vano aborda, sin ir más lejos, la problemática de la receta electrónica, asunto que durante estos días precisamente, es objeto de un arduo debate en los medios de comunicación nacionales bajo titulares mediáticos del tipo: "Éste será el primer verano (el de 2019) en el que la receta electrónica será interoperable en todas las Comunidades Autónomas de España". En concreto, es el Capítulo cuarto de la Primera Parte, el que se destina al examen de documentos digitales tales como la receta y tarjeta sanitaria digitales. Paralelamente estudia el fenómeno tan en boga últimamente del denominado "Big Data", ya muy afincado en nuestra terminología, asumiendo un mayor grado de complejidad al circunscribirse en el espinoso campo de la salud, siendo la peculiaridad de que se compone de información personal y sensible de las personas lo cual cobra, insisto, aún más magnitud.

Por todo lo dicho hasta ahora, la lectura de la monografía de la Dra. Cristea deviene prácticamente obligatoria para todos aquéllos que tengan interés en estudiar y discutir, desde un enfoque jurídico, una gran variedad de temas relacionados con el derecho a la protección de datos de salud. Se trata, por ende, de una obra de amplio espectro que no obstante lo anterior, tiene el mérito de ofrecer una perspectiva completa, sencilla y primorosamente ordenada de este *sui generis* sector, que lo convierte en tan interesante como difícilmente abarcable, si se pretende exhaustividad en un monográfico que como éste, es de carácter eminentemente práctico.

El pilar sobre el que se sostiene esta sólida monografía reside en la imperiosa necesidad del reconocimiento del derecho a la protección de datos como un nuevo derecho fundamental en la esfera normativa, tanto en el ámbito nacional como europeo, carente en la actualidad de una regulación específica, uniforme, consolidada y actualizada. Añadiendo un grado mayor de complejidad a la tesis, la presente obra tiene por objeto el estudio de las fuentes normativas referentes a la protección de los datos de salud (que, recalcamos, son datos sensibles o especialmente protegidos) tanto en el ámbito de la Unión Europea como en el ámbito nacional y autonómico así como el análisis del cambio de paradigma que se vislumbra en el contexto del *Big Data* en el ámbito sanitario, que entra en colisión con la protección al derecho de intimidad y la confidencialidad de los datos de salud.

Como advierte la propia autora en el capítulo introductorio, su investigación se ha desarrollado valiéndose de los instrumentos propios de la metodo-

logía jurídica. En primer lugar, desde la observación pragmática y descriptiva del uso de datos, mecanismos de recogida, del tratamiento y acerca de su utilización. En segundo lugar, y desde la perspectiva de investigación pura, se ha focalizado en la selección y desgranaje de la legislación existente en la materia, tanto en el horizonte europeo como nacional, en el análisis de las diversas opiniones doctrinales de referencia, en la jurisprudencia, en los informes del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE y en los informes y resoluciones de las Agencias de Protección de Datos. En tercer orden, y desde un punto de vista analítico, se ha embarcado en la espinosa tarea de interpretar si la legislación existente en cuestión de protección de datos, ofrece o no respuesta a la utilización y al tratamiento de los mismos, y, en consecuencia, si tutela nuestros datos personales.

Para afrontar este tema de investigación, la monografía se estructura en dos Partes. La Primera se divide en cuatro Capítulos. El primero de éstos presenta un carácter más introductorio y un enfoque más conceptual. De tal forma, la autora comienza con la definición de los conceptos objeto del análisis a lo largo de esta obra, identificando cuál es el bien jurídico protegido por el derecho, en pro de poder analizar concienzudamente qué es un dato, diferenciándolo de otras imprecisiones terminológicas, acotando el objeto de estudio para centrarse en el contenido de los datos sensibles incidiendo en los datos de salud.

En el segundo Capítulo de la Primera Parte, comienza su análisis desentrañando los elementos jurídicos que vinculan a los datos de salud, estudiando en profundidad los principios jurídicos y éticos, que deben observarse a la hora del tratamiento de esta categoría de datos, por parte del facultativo médico y del personal sanitario, para explicar los derechos que le asisten al interesado en relación con sus datos de salud y las sanciones que el ordenamiento jurídico prevé en caso de su incumplimiento. La Profesora Cristea se revela como una analista concienzuda que sistematiza qué se entiende por tratamiento de los datos personales y cuáles son sus límites normativos, en la medida en que –como ella misma subraya– los datos por sí mismos no constituyen ningún riesgo. Lo que sí goza de amparo normativo es su tratamiento, y así estima, con tino, analizar. Es decir, el hecho de que nuestros datos personales sean tratados por terceras personas supone un peligro, y este denominado "tratamiento" es lo que exige un marco legal y ético sobre el que ahonda en este Capítulo segundo de su libro.

El tercer Capítulo vertebra esta Primera Parte de su obra y en él la autora examina la integración de los datos de salud que se encuentran comprendidos

en la historia clínica del paciente. En este Capítulo se adentra, con las herramientas que le ofrece el Derecho, en los requisitos que deben observarse en torno a la historia clínica. Así las cosas, acomete un breve repaso a su origen, a su definición y a los aspectos que debe reunir, a su contenido, intentando deslindar los parámetros jurídicos que la historia clínica debe respetar, como eje de la relación médico-paciente.

El Capítulo cuarto de la Primera Parte, profundiza, desde un enfoque jurídico y social en las polémicas más actuales, lo que imprime una visión fresca e innovadora al centrarse en profundizar y analizar, a través de la incorporación de las nuevas tecnologías, la evolución que se ha vislumbrado en las últimas décadas en lo atinente a las especificidades que la digitalización incorpora en la historia clínica digital, su funcionalidad, los datos que debe contener, las medidas de seguridad que debe respetar y las responsabilidades de los intervinientes en su consulta y redacción.

En la Segunda Parte del libro, en el Capítulo primero, la autora hace referencia al cambio de modelo económico y social con respecto al incremento del intercambio transfronterizo de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas, como resultado de la aceleradísima evolución tecnológica y la globalización, siendo estos elementos los que plantean nuevos retos para la protección de los datos personales tanto en la órbita europea como nacional.

Paralelamente, esta parte de la obra se adentra en analizar y valorar los resultados de la significativa iniciativa normativa de UE, con la reciente aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta nueva ordenación legal, que ha entrado en vigor el 25 de mayo del año 2018, ha derogado la mítica Directiva 95/46/CE. El Reglamento General de Protección de Datos, introduce varias novedades englobadas en un nuevo modelo de protección de datos para Europa. Entre sus previsiones, entresaca la autora el cambio en la gestión de los datos y el uso responsable de la información. Esto, preconiza, que conllevará dar un mayor protagonismo a una figura de nueva creación que es el Delegado de Protección de Datos, en el que recaerá la responsabilidad de determinar y adoptar las medidas que sean necesarias para garantizar la adecuada protección de los datos. Resulta forzoso señalar que el Reglamento introduce en el campo de los datos de salud, dos nuevas categorías, tales como los datos biométricos y los datos genéticos. También reformula algunos de los

principios que inspiran la protección de datos y suscribe otros nuevos, así como realiza otras aportaciones novedosas que la Dra. Cristea desgrana en este Capítulo.

Como cierre, el Capítulo II de la Segunda Parte, nos ofrece un estudio del fenómeno, en auge, del *Big Data* sanitario, analizando las ventajas que brinda unificar la información sanitaria dispersa que se dispone de cada paciente y en diversos formatos, agrupándola y organizándola de forma tal, que redunde no sólo en beneficio del paciente sino también para el sector médico, para la organización hospitalaria,y para las farmacéuticas. No escatima la Profesora Cristea en analizar los inconvenientes que se intuyen en la implementación del *Big Data* en salud, entre los que destacan la anonimización de los datos que se muestra ajena y no es garantía de la no re-identificación de las personas, creando vulnerabilidad en torno a la información, y la necesidad de que la recopilación, el almacenamiento, el tratamiento y la confidencialidad de los datos sensibles quede garantizada, dotando de mayores garantías jurídicas a la protección de los datos de salud en este novedoso pero ineludible entorno tecnológico.

En definitiva, el propio interés que suscita la obra, incita a reflexionar sobre una cuestión sobre la que incide su autora: la necesidad de la concepción de una nueva rama del derecho, esto es, el Derecho Sanitario, sobre la base de que el derecho a la salud posee un espectro demasiado amplio que toca la rama del derecho civil, administrativo, laboral, penal y constitucional y ello conlleva a que su regulación sea muy dispersa, fragmentaria e ineficiente. Por ello, sostiene que cada vez es más notorio el requerimiento de independizar al derecho sanitario y convertirlo en una nueva rama del derecho. Reflexiones que suscita la lectura de un buen trabajo que puede resultar de gran importancia para los operadores jurídicos, especialmente necesario en un ámbito tan sensible como la protección de datos de salud. Ámbito donde, efectivamente, la seguridad, el contenido y la manipulación o tratamiento de nuestros datos sensibles tiene un gran futuro y también un largo camino por recorrer.

Estimo, y ello es lo más importante, que es razonable afirmar que estamos ante una de las obras que, dentro de la doctrina de la especialidad que, durante estos últimos años vienen apareciendo *in crescendo*, ofrece aportaciones personales, sin limitarse, como no pocas veces ocurre, a exponer lo ya dicho y escrito por otros, incluso con gran proximidad en el tiempo. De tal manera que la autora no se limita a informarnos exhaustivamente de los

riesgos que el *Big Data* nos puede acarrear, sino que nos ofrece soluciones para paliar estos problemas.

Dra. Elena Atienza Macías

Doctora en Derecho por la Universidad de Deusto

Investigadora Postdoctoral "Juan de la Cierva" en la Universidad del País Vasco UPV/EHU

Grupo de Investigación Cátedra de Derecho y Genoma Humano

Referencias bibliográficas y documentales*

*References to books, articles in periodicals and to other documents***

1. Libros / Books

AA.VV., *Big Data, Health Law, and Bioethics,* Cohen, I. Glenn / Fernandez Lynch, Holly / Vayena, Effy / Gasser, Urs (Eds.), Cambridge University Press, Cambridge, Reino Unido, 2018.

AA.VV., *Tratado de Protección de Datos,* Rallo Lombarte, Artemi (Dir.), Ed. Tirant Lo Blanch, Valencia, España, 2019.

AA.VV., *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Coord.), Ed. Thomson Reuters, Cizur Menor, España, 2019.

AA.VV., *El cuerpo diseminado: estatuto, uso y disposición de los biomateriales humanos,* García Manrique, Ricardo (Coord.), Ed. Aranzadi, Cizur Menor, España, 2018.

AA.VV., *Blockchain in Healthcare: Innovations that Empower Patients, Connect Professionals and Improve Care,* Productivity Press, Nueva York, Estados Unidos de América, 2019.

Andreu Martínez, María Belén, *La autonomía del menor en la asistencia sanitaria y el acceso a la historia clínica*, Ed. Aranzadi, Cizur Menor, España, 2018.

Cristea Uivaru, Lucía, *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud,* Ed. Bosch, Barcelona, España, 2019.

* Para incluir referencias en esta Sección se remitirá un ejemplar de la publicación correspondiente a la Dirección de la Revista.

** Persons wishing to include references in this Section are asked to forward a copy of the publication in question to the Editor of the Review.

Delgado Carravilla, Enrique / Puyol Montero, Javier, *La Implantación del Nuevo Reglamento General de Protección de Datos de la Unión Europea,* Ed. Tirant lo Blanch, Valencia, España, 2018.

García San José, Daniel, *La Europa de los Derechos Ante los Avances Científicos y Tecnológicos,* Ed. Tirant Lo Blanch, Valencia, España, 2018.

Gudín Rodríguez-Magariños, Faustino, *Nuevo Reglamento europeo de protección de datos versus Big Data,* Ed. Tirant lo Blanch, Valencia, España, 2018.

Jiménez Asensio, Rafael, *Introducción al nuevo marco normativo de la protección de datos personales en el sector público,* Ed. IVAP, Oñati, España, 2019.

Ortega Giménez, Alfonso, *Las aplicaciones del Big Data en el ámbito asegurador y el tratamiento legal de sus datos, Una perspectiva desde el derecho internacional privado,* Fundación MAPFRE, Madrid, España, 2019.

Ottolia, Andrea, *Derecho, Big Data e Inteligencia Artificial*, Ed. Tirant Lo Blanch, Valencia, España, 2018.

Puyol , Javier, *Delegado de Protección de Datos (DPO) Dominio 1,* Ed. Tirant Lo Blanch, Valencia, España, 2019.

Recio Gayo, Miguel, *Protección de datos personales e innovación: ¿(in) compatibles?,* Ed. Reus, Madrid, España, 2018.

Rueda Martín, María Ángeles, *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Ed. Atelier, Barcelona, España, 2018.

2. Artículos de Revista / Articles in Periodicals

AA.VV., "El nuevo Reglamento Europeo sobre Protección de Datos y su aplicación sobre el Derecho ARCO en sanidad", *Cuidados, aspectos psicológicos y actividad física en relación con la salud*, Pérez-Fuentes, María del Carmen (comp.), Gázquez Linares, José Jesús, (comp.), Molero Jurado, María del Mar (comp.), Barragán Martín, Ana Belén (comp.), Martos Martínez, África (comp.), Simón Márquez, María del Mar (comp.), Asociación Universitaria de Educación y Psicología (ASUNIVEP), 2018, pp. 557-562.

Alarcón Sevilla, Verónica, "Actualización de la normativa de protección de datos en materia de sanidad: su incidencia en salud pública e investigación de enfermedades", *Autonomía del paciente mayor, vulnerabilidad y e-salud*, Andreu Martínez, María Belén / Salcedo Hernández, José Ramón (Coords.), Ed. Tirant lo Blanch, Valencia, España, 2018, pp. 255-274.

Álvarez Rigaudias, Cecilia, "Tratamiento de datos con fines de investigación científica y/o médica", *Tratado de Protección de Datos,* Rallo Lombarte, Artemi (Dir.), Ed. Tirant Lo Blanch, Valencia, España, 2019, pp. 672-707.

Atienza Macías, Elena, "Big data y medicina personalizada: oportunidades para el sistema sanitario en relación con el envejecimiento de la población. Especial referencia al nuevo panorama normativo europeo de protección de datos", *Envelhecimento (Colecção Escritos de Direito da Saúde, Núm. 2),* Pereira, André Dias (Coord.), Edição FAF - Sociedade de Advogados, Coimbra-Lisboa, Portugal, 2018, pp. 107-125.

Benlloch Domènech, Cristina / Sarrión Esteve, Joaquín, "eSalud-administración sanitaria digital", *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Ed. Thomson Reuters Aranzadi, Cizur Menor, España, 2018, pp. 499-529.

Burke, W. / Beskow, L.M. / Trinidad, S. B. *et ál.,* "Informed Consent in Translational Genomics: Insufficient Without Trustworthy Governance", *The Journal of Law, Medicine & Ethics* [en línea]. Núm. 1, Vol. 46, 2018, pp. 79-86.

Casanova Asencio, Andrea Salud, "Protección de datos en el ámbito de la historia clínica:: el acceso indebido por el personal sanitario y sus consecuencias", *Indret: Revista para el Análisis del Derecho*, Núm. 2, 2019.

Chico, V., "The impact of the General Data Protection Regulation on health research", British Medical Bulletin, Núm. 1, Vol. 128, 2018, pp. 109-118.

Chieffi, L., "La tutela della riservatezza dei dati sensibili: le nuove frontiere europee", *federalismi.it*., Núm. 4, 2018, pp. 1-52.

Colcelli, Valentina, "Information on Access and Benefit Sharing regarding the Utilisation of Genetic Resources under the European Union Legal Regulation", *Genetic Information and Individual Rights*, Regensburg Universitat, Berlín, Alemania, 2018.

Cook-Deegan, R. / Majumder, M. A. / Mcguire, A. L., "Introduction: Sharing Data in a Medical Information Commons", *The Journal of Law, Medicine & Ethics*, Núm. 1, Vol. 47, 2019 pp. 7-11.

Crespí Ferriol, María Del Mar, "El tratamiento de los datos personales relativos a la salud de los trabajadores", *Revista General de Derecho del Trabajo y de la Seguridad Social*, Núm. 52, 2019, pp. 257-298

De Lecuona, Itziar, "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (*big data*)", *Gaceta Sanitaria,* Núm. 6, Vol. 32, 2018, pp. 576-578.

De Lecuona, Itziar, "El valor y el precio de los datos personales de salud en la sociedad digital", *El cuerpo diseminado: estatuto, uso y disposición de los biomateriales humanos,* García Manrique, Ricardo (Coord.), Ed. Aranzadi, Cizur Menor, España, 2018, pp. 171-190.

De Lecuona, Itziar / Villalobos-Quesada, María, "European Perspectives on Big Data Applied to Health: the Case of Biobanks and Human Databases", *Developing World Bioethics,* Núm. 3, Vol. 18, 2018, pp. 291-298.

Delvaux, Nicolas / Aertgeerts, Bert *et. ál*, «Health Data for Research Through a Nationwide Privacy-Proof System in Belgium: Design and Implementation", *JMIR Medical Informatics*, Núm. 4, Vol. 6, octubre-diciembre 2018. pp. 219-228.

Díaz García, Juan "Implantación de la figura del Delegado de Protección de Datos en el Sistema Nacional de Salud", *I+S: Revista de la Sociedad Española de Informática y Salud,* Núm. 134, 2019, pp. 66-66.

Díaz, Juan "Las evaluaciones de impacto de privacidad en los entornos sanitarios", *I+S: Revista de la Sociedad Española de Informática y Salud*, Núm. 135, 2019, pp. 75-75.

Donnelly, M., / Mcdonagh, M., "Health Research, Consent and the GDPR Exemption". *European Journal of Health Law,* Núm. 2, Vol. 26, 2019, pp. 97-119.

Dopazo Fraguío, Pilar, "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (novedades del Reglamento General de Protección de Datos)", *Revista española de derecho europeo,* Núm. 68, 2018, pp. 113-148.

Dove, E., "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era", *The Journal of Law, Medicine & Ethics*, Núm. 4, Vol. 46, 2018, pp. 1013-1030.

Elvy, Stacy-Ann, "Commodifying consumer data in the era of the internet of things", *Boston College Law Review*, Núm. 2, Vol. LIX, 2018, pp. 423-522.

Escribano Cañas, Blanca, "Dos proyectos de Reglamento europeos mantienen en vilo a la llamada 'economía de los datos' de la Unión", *Actualidad Jurídica Aranzadi*, Núm. 937, 2018.

Fernow, Josepine / De Miguel Beriain, Iñigo / Brey, Philip / Stahl, Berndt *et ál.,* "Setting future ethical standards for ICT, Big Data, AI and robotics: The contribution of three European projects", *Orbit Journal,* 2019.

García, Rafael, "El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario", *I+S: Revista de la Sociedad Española de Informática y Salud,* Sociedad Informática de la Salud, Núm. 127, 2018, pp. 13-20.

Kalkman, Shona *et ál.,* "Responsible data sharing in international health research: a systematic review of principles and norms", *BMC Medical Ethics,* Vol. 20, artículo nº 21, Marzo de 2019.

Lizarraga Bonelli, Emilio, "Protección de datos y asistencia médica: hacia un nuevo paradigma del consentimiento", *Actualidad del derecho sanitario*, Núm. 270, 2019, pp. 469-472.

Lomas Hernández, Vicente, "Principales novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desde la perspectiva sanitaria", *I+S: Revista de la Sociedad Española de Informática y Salud,* Núm. 134 2019, pp. 7-11.

Nicolás Jiménez, Pilar, "Investigación biomédica y *bigdata* sanitarios", *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal,* Troncoso Reigada, Antonio (Coord.), Ed. Thomson Reuters, Cizur Menor, España, 2019.

Nicolás Jiménez, Pilar / Fernández De Uzquiano, Emma / Alfonso Farnós, Iciar, "Biobank External Ethics Committees (BEEC) in Spain. Nature, functions and operating procedures", *BioLaw Journal – Rivista di BioDiritto*, Núm. 2, 2018, pp. 205-216.

Mostert, Menno / Bredenoord, Annelien L. / Van Der Slootb, Bart / Van Deldena, Johannes J.M., *From Privacy to Data Protection in the EU: Implications for Big Data Health Research*, *European Journal of health law*, Vol. 25, 2018, pp. 43-55.

Pérez Gómez, José María, "Breve aproximación a la incidencia del nuevo marco regulatorio del RGPD en el ámbito sanitario (II)", *Actualidad del Derecho Sanitario*, Núm. 261, 2018, pp. 743-745.

Pérez Luño, Antonio Enrique, "El derecho a la intimidad y la protección de los datos personales biomédicos", *Democracia, pluralismo y derechos humanos: 500 años,* Sánchez Bravo, Álvaro A. (Dir.), Facultad de Derecho, Universidad de Sevilla. X años de Encuentros hispanos-brasileños de filosofía del derecho y derechos humanos, 2019, pp. 25-49.

Pinedo García, Igor, "El Reglamento Europeo de Protección de Datos y las oficinas de farmacia", *Revista Aula de Farmacia*, Septiembre – Octubre 2018, pp. 40-43.

Quinn, P. / Liam, Q., "Big genetic data and its big data protection challenges", *Computer Law & Security Review***,** Núm. 5, Vol. 34, Octubre 2018, pp. 1000-1018.

Romeo Casabona, Carlos María, "El nuevo marco normativo europeo sobre protección de datos personales y el estatuto de las muestras biológicas humanas y de los biobancos para investigación biomédica", *Comunicaciones en propiedad industrial y derecho de la competencia,* Núm. 86, 2019, pp. 215-238

Rubí Navarrete, Jesús, "Novedades sobre la investigación sanitaria: el Dictamen 3/2019 del Comité Europeo de Protección de Datos", *Comunicaciones en propiedad industrial y derecho de la competencia,* Núm. 86, 2019, pp. 5-18.

Sarrión Esteve, Joaquín, "Health Data Treatment: An approach to the International and EU Legal Framework", *Genetic Information and Individual Rights*, Arnold, Rainer / Cippitani, Roberto (Eds.), Regensburg Universitat, Berlín, Alemania, 2018. pp. 36-53.

Sarrión Esteve, Joaquín, "The problem of the consent for the processing of health data, particularly for biomedical research purposes, from the perspective of fundamental rights protection in the Digital Era", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine,* Núm. 48, 2018, pp. 107-132.

Shabani, M. / Borry, P., "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation", *European Journal of Human Genetics,* Núm. 2, Vol. 26, 2018, pp.149-156.

Troncoso Reigada, Antonio, "La seguridad en el Reglamento General de Protección de Datos de la Unión Europea", *Actualidad administrativa*, Núm. 1, 2019.

Troncoso Reigada, Antonio, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada / Law and The Human Genome Review: Genetics, Biotechnology and Advanced Medicine*, Núm. 49, 2018, pp. 187-266.

Ustarán, Eduardo / García, Paula, "Transferencias internacionales de datos", *Tratado de Protección de Datos*, rallo lombarte, Artemi (Dir.), Ed. Tirant Lo Blanch, Valencia, España, pp. 432-459.

Van Been, Evert-ben, "Observational health research in europe: understanding the general data protection regulation and underlying debate", *European Journal of Cancer*, Elsevier y European Organisation for Research and Treatment of Cancer, Vol. 104, 2018, pp. 70-80.

Vayena, E. / Blasimme, A., "Health Research with Big Data: Time for Systemic Oversight", *The Journal of Law, Medicine & Ethics*, Núm. 1, Vol. 46, 2018, pp. 119-129.

Vázquez De Castro, Eduardo, "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Núm. 46, 2018.

Zeng, Jing / Glaister, Keith W., "Value creation from big data: Looking inside the black box", *Strategic Organization*, Núm. 2, Vol. XVI, 2018, pp. 105-140.

3. Otros documentos / Other documents

Agencia Española de Protección de datos (AEPD), *Informe 073667/2018 de la AEPD sobre la incidencia en el ámbito de la investigación biomédica del RGPD,* 2018. Disponible en: https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

Autoritat Catalana de Protecció de Dades (APDCAT), *Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomèdica,* Mayo 2019. Disponible en: https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/Documents/ca_cns_2019_015.pdf

Autoritat Catalana de Protecció de Dades (APDCAT), *Dictamen en relació amb la consulta d'una associació de l'àmbit sanitari sobre diferents aspectes relacionats amb l'apartat 2 de la disposició adicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals*, Mayo 2019. Disponible en: https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2019/Documents/ca_cns_2019_018.pdf

European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)),* Enero 2019. Disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf

European Data Protection Board, EDPB-EDPS *Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI),* Julio 2019. Disponible en: https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_en.pdf

International Conference of Data Protection & Privacy Commissioners (ICDPPC), *Declaration on Ethics and Data Protection in Artificial Intelligence,* 40th International Conference of Data Protection and Privacy Commissioners, Bruselas, Bélgica, octubre 2018. Disponible en: https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS), "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", Beltrán Aguirre, José Luis / García López, Fernando José / Navarro Sánchez, Carmen, Sociedad Española de Salud Publica y Administración Sanitaria, Barcelona, España, Noviembre 2017. Disponible en: https://sespas.es/wp-content/uploads/2018/02/SESPAS_informe_proteccion_datos_2017.pdf

4. El Genoma Humano en la red / The Human Genome in the net

G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU: www.catedraderechoygenomahumano.es

Portal de publicaciones en línea de la Cátedra: www.bioderecho.eu

Enciclopedia de Bioderecho y Bioética, G.I. Cátedra de Derecho y Genoma Humano, Universidad del País Vasco UPV/EHU / Fundación Instituto Roche: www.enciclopedia.bioderecho.com

Basque Cybersecurity Centre - BCSC
https://www.basquecybersecurity.eus/

Cátedra Google de Privacidad, Sociedad e Innovación, Fundación Universitaria San Pablo CEU
https://www.uspceu.com/investigacion/catedras-investigacion/google

European-Canadian Cancer Network (EUCANCan)
https://eucancan.com/

EuroBioBank
http://www.eurobiobank.org/

European '1+ Million Genomes' Initiative, Digital Single Market, European Commission
https://ec.europa.eu/digital-single-market/en/european-1-million-genomes-initiative

European Data Protection Board (EDPB)
https://edpb.europa.eu/

European Group on Ethics in Science and New Technologies
http://ec.europa.eu/european_group_ethics/index_en.htm

PANELFIT, Participatory Approaches to a New Ethical and Legal Framework for ICT
https://www.panelfit.eu/

Proyecto BIFAP, Base de datos para la Investigación Farmacoepidemiológica en Atención Primaria
http://www.bifap.org/
Proyecto BigdatIus, Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos "Oportunidades e implicaciones jurídicas"
http://www.bigdatius.com/
Proyecto MIDAS, *Meaningful Integration of Data, Analytics and Services*
www.midasproject.eu
SIENNA project (Stakeholder-Informed Ethics for New technologies with high socio-ecoNomic and human rights impAct)
http://www.sienna-project.eu/about-sienna/
The Big Data Institute (BDI), Li Ka Shing Centre for Health Information and Discovery, University of Oxford's Old Road Campus
https://www.bdi.ox.ac.uk/
The Centre for health, Law and Emerging Technology (HeLEX), University of Oxford
http://www.dph.ox.ac.uk/helex
The Global Alliance for Genomics and Health (GA4GH)
https://www.ga4gh.org/
The ICGC ARGO Project (Accelerating Research in Genomic Oncology)
https://icgc-argo.org/

.

NORMAS DE PUBLICACIÓN PARA LOS AUTORES

1.- TEMAS DE INTERÉS E IDIOMA DE LA PUBLICACIÓN

En la «Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine» se integran trabajos de especialistas cualificados de centros de investigación nacionales y extranjeros y de profesionales de reconocido prestigio, quienes aportan sus reflexiones y puntos de vista sobre las **cuestiones jurídicas que plantea la genética humana, la biotecnología y la medicina avanzada,** garantizando la imprescindible libertad de pensamiento y la pluralidad de enfoques e ideas bajo un planteamiento multidisciplinar, con sólida base científica y biotecnológica, ético-filosófica, humanística y social.

La comunicación científica que pretende canalizar la Revista es bidireccional: que los autores extranjeros más relevantes sean conocidos en nuestro país y, a la inversa, que los españoles puedan ser conocidos y leídos tanto en nuestro país como en el extranjero. Esta amplia difusión, reforzada por su carácter de **publicación bilingüe** (con trabajos **en c**astell **ano y en inglés**) pretende acercar las distintas perspectivas.

2.- TRABAJOS ORIGINALES Y DE CARÁCTER INÉDITO

Los trabajos que se remitan para su publicación en la «Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine» **deberán ser inéditos y no estar pendientes de publicación** en otra Revista. No obstante, una vez aparecidos en la «Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine» podrán ser publicados en otro lugar.

3.- ENVÍO DE ORIGINALES

La periodicidad de la Revista es semestral (constando de dos ediciones: Número Enero-Junio y Número Julio-Diciembre) con alrededor de 250 páginas cada una, y con las siguientes secciones fijas: **Opinión, Doctrina, Jurisprudencia** (con comentarios), **Informes, Documentos y Bibliografía** (con recensiones y referencias bibliográficas, documentales y enlaces de internet a páginas de interés).

Todas las secciones de la Revista están abiertas a quienes deseen colaborar en la misma para suscitar el intercambio de ideas, puntos de vista e información que faciliten la obtención de criterios o enfoques compartidos.

Los trabajos se enviarán por correo electrónico a la Dra. Aitziber Emaldi Cirión: aitziber.emaldi@deusto.es y a la Dra. Elena Atienza Macías: elena.atienza@ehu.eus (consultar fechas de recepción con las coordinadoras).

4.- FORMATO

Los originales deberán ir escritos a espacio simple, en **letra Arial, tamaño 10 en texto y 9 en las notas a pie de página.**

El trabajo irá encabezado por su título y debajo del mismo, se colocará el nombre y apellidos del autor o autores, profesiones o cargos que deberán figurar en la publicación (**filiación académica**) e institución a la que pertenezcan.

Seguidamente se deberá acompañar el sumario del artículo, un **breve resumen** del contenido del mismo (con una extensión aproximada de 350 caracteres) en castellano y en inglés, es imprescindible que se realice una relación de **palabras clave** (como mínimo 5) indicativas de lo tratado en el trabajo, en castellano y en inglés.

Citas y referencias bibliográficas:

- Se debe seguir el siguiente modelo (según se trate de artículo de revista o monografía):

ROMEO CASABONA, Carlos María, «La cuestión jurídica de la obtención de células troncales embrionarias humanas con fines de investigación biomédica. Consideraciones de política legislativa», *Revista de Derecho y Genoma Humano / Law and the Human Genome Review,* Núm. 24, Vol. 1, 2006, pp. 75-100.

BUIJSEN, Martin / DEN EXTER, André, «Equality and the Right to Health Care», *Human Rights and Biomedicine*, DEN EXTER, André (Ed.), Maklu Publishers, the Netherlands, 2010, p. 75.

ROMEO CASABONA, Carlos María, *Los genes y sus leyes. El Derecho ante el genoma humano*, Ed. Cátedra Interuniversitaria de Derecho y Genoma Humano — Comares, Bilbao-Granada, España, 2002, pp. 100 -102.

- En los documentos electrónicos: Se incluye el nombre de la base de datos consultada. A la referencia correspondiente según el tipo de documento se añadirá "Disponible en: http://xxxxxx", con la fecha de consulta, y a continuación del DOI, si lo hubiere.

La Declaración de Helsinki y sus sucesivas modificaciones pueden ser consultadas *on line* en la web oficial de la Asociación Médica Mundial disponible en: http://www.wma.net/s/policy/pdf/17c.pdf [Última consulta: 15 de agosto de 2012].

- Como alternativa o complemento de las notas a pie de página, podrá incluirse al final una breve referencia bibliográfica orientativa sobre la materia objeto de estudio en el trabajo. La veracidad de las citas y referencias bibliográficas será responsabilidad del autor o autores del artículo.

Figuras y tablas:

- Deben enviarse en ficheros aparte. Llevarán un encabezamiento conciso e irán numeradas; las tablas con números romanos y las figuras con arábigos. Las figuras deben ser en blanco y negro. Se debe especificar en el texto la posición aproximada de las figuras y tablas. Los formatos serán TIFF o JPEG con una resolución mínima de 300 ppp. Los gráficos y dibujos se presentarán en archivos vectoriales. Toda ilustración debe tener un pie de foto, y cada tabla un título identificativo. Los autores son responsables de obtener los oportunos permisos para reproducir material (texto, tablas o figuras) de otras publicaciones o de otra procedencia (bibliotecas, archivos…) y de citar correctamente dicha procedencia.

5.- EXTENSIÓN

La extensión máxima fijada para los trabajos es de **50.000 caracteres.** Excepcionalmente, en atención al posible interés y calidad del contenido del trabajo aportado, las limitaciones señaladas de extensión máxima podrán sobrepasarse, siempre y cuando el Consejo científico —interno y externo— de la Revista considere que el exceso es razonable.

6.- PROCESO DE PUBLICACIÓN

A todos los autores que envíen originales a la «Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine» se les remitirá acuse de recibo.

El Comité de Redacción someterá previamente los trabajos a dos evaluaciones anónimas —interna y externa— y decidirá, en un plazo no superior a los dos meses, la aceptación o no de los trabajos recibidos. Esta decisión se comunicará al autor. En caso de rechazarse la publicación, esta decisión le será comunicada al interesado por correo electrónico o, en su caso, por correo postal. En dicha notificación se le expondrán los motivos que han conducido a la negativa. En caso afirmativo, se indicará volumen y número de la Revista en el que se publicará.

PUBLICATION RULES FOR AUTHORS

1.-TOPICS OF INTEREST AND LANGUAGE OF PUBLICATION

The «Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine / Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada» contains works by qualified specialists from national and foreign research centres and by professionals of renowned excellence, who provide their opinions and view points on **legal issues posed by human genetics, biotechnology and advanced medicine,** guaranteeing the essential freedom of thought and the multiple approaches and ideas under a multidisciplinary approach, with a solid scientific, biotechnological, ethical-philosophical, humanistic and social basis.

The scientific communication which the Review intends to channel is twofold: that the most significant foreign authors are recognised in our country and, conversely, that Spanish authors are recognised and read both in Spain and abroad. This extensive publication, backed up by the fact that it is a **bilingual publication** (with works **in Spanish and English**) aims to bring different perspectives together.

2.- ORIGINAL AND UNPUBLISHED WORKS

Those works submitted for publication in the «Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine / Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada» **must be unpublished and not pending publication** in any other Review. However, once they feature in the «Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine / Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada» they may be published in another place.

3.- SENDING ORIGINALS

The Review is biannual (with two editions: a January-June issue and a July-December issue) each of about 250 pages, with the following set sections: **Opinion, Articles, Case Law Notes** (with commentaries), **Reports, Documents and Bibliography** (with reviews and bibliographic and documentary references and internet links to sites of interest).

All sections of the Review are open to those who wish to collaborate in it to bring about the exchange of ideas, points of view and information which allows shared criterion or approaches to be obtained.

Papers will be sent by email to Dr. Aitziber Emaldi Cirión: aitziber.emaldi@deusto.es and to Dr. Elena Atienza Macías: elena.atienza@ehu.eus (check receipt dates with coordinators).

4.- FORMAT

The originals must be written in single spacing, **Arial font, size 10 text and 9 for footnotes.**

The work should have a title at the top, below which the name and surname, profession or positions of the author(s) should appear in the publication (**academic affiliation**) and the institution to which they belong.

Immediately below there should be the summary of the article, an **abstract** of the content thereof (of approximately 350 characters in length) in Spanish and in English. It is essential that a list of **keywords** are provided (at least 5) which are indicative of the subject matter, in Spanish and in English.

Quotes and bibliographic references:

- The following layout should be followed (depending on whether a review article or an authors' monograph is involved):

ROMEO CASABONA, Carlos María, "La cuestión jurídica de la obtención de células troncales embrionarias humanas con fines de investigación biomédica. Consideraciones de política legislativa", *Law and the Human Genome Review / Revista de Derecho y Genoma Humano,* No. 24, Vol. 1, 2006, pp. 75-100.

BUIJSEN, Martin / DEN EXTER, André, "Equality and the Right to Health Care", *Human Rights and Biomedicine*, DEN EXTER, André (Ed.), Maklu Publishers, the Netherlands, 2010, p. 75.

ROMEO CASABONA, Carlos María, *Los genes y sus leyes. El Derecho ante el genoma humano*, Ed. Cátedra Interuniversitaria de Derecho y Genoma Humano — Comares, Bilbao-Granada, Spain, 2002, pp. 100 -102.

- In electronic documents: the name of the database consulted is included. To the corresponding reference depending the type of the document will be added: "Available at: http://xxxxxx" with the consultation date, and then the DOI, if it would exist.

The Helsinki Declaration and its amendments can be consulted on line at the official website of the World Medical Association available at: http://www.wma.net/s/policy/pdf/17c.pdf [Last accessed: 15 August 2012].

- As an alternative or complement to the footnotes, a brief illustrative bibliography may be included on the material studied for the work. The accuracy of the quotations and references will be the responsibility of the author.

Figures and Tables:

• They are to be submitted in separate files. They should be numbered and have a concise heading: The tables are to be in Roman numerals and Arabic figures. The figures should be set in black and white. The approximate position of the figures and tables are to be specified in the text. The formats should be TIFF and JPEG with a minimum resolution of 300 dpi. The Graphics and drawings are to be submitted in vector files. Each illustration should have a caption and each table an identifying title. Authors are responsible for obtaining authorisation for reproduction material (text, tables or figures) from other publications or other sources (libraries, archive…) and properly cite said source.

5.- LENGTH

The maximum established length for works is **50.000 characters.** Exceptionally, in view of possible interest and quality of the content of the work provided, the maximum length established may be exceeded, so long as the Scientific Board —internal and external— of the Review deem the excess is reasonable.

6.- PUBLICATION PROCESS

All authors who send originals to the «Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine / Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada» will receive an acknowledgement slip.

The Editorial Committee shall subject all works to two anonymous evaluations —internal and external— and will decide, within a period not exceeding two months, on the acceptance or rejection of works received. The author will be informed of this decision. In the event that the publication is rejected, the interested party will be advised of this by email or, when applicable, by post. The notification will state the reasons for rejection. In the event that it is accepted, the volume and number of the Review in which it will be published will be indicated.

PUBLICACIONES / PUBLICATIONS

LIBROS / BOOKS

- *Genética Humana. Fundamentos para el estudio de los efectos sociales de las investigaciones sobre el genoma humano*, C. M. Romeo Casabona (Ed.), Bilbao, 1995, 357 pp.

En Coedición con Ed. Comares (Granada):

- *Código de Leyes sobre Genética*, C.M. Romeo Casabona (Ed.), 1997, 886 pp.
- *Biotecnología y Derecho. Perspectivas en Derecho Comparado,* C.M. Romeo Casabona (Ed.), 1998, 405 pp.
- *Eugenesia hoy,* C.M. Romeo Casabona (Ed.), 1999, 372 pp.
- *Genética y Derecho Penal,* C.M. Romeo Casabona (Ed.), 2001, 390 pp.
- Mora Sánchez, Juan Miguel, *Aspectos sustantivos y procesales de la tecnología del ADN*, 2001, 378 pp.
- Emaldi Cirión, Aitziber, *El consejo genético y sus implicaciones jurídicas*, 2001, 543 pp.
- *El Convenio de Derechos Humanos y Biomedicina del Consejo de Europa: su entrada en vigor en el ordenamiento jurídico español*, C.M. Romeo Casabona (Ed.), 2002, pp. 544.
- Romeo Casabona, Carlos María, *Los genes y sus leyes*, 2002, 273 pp.
- *Características biológicas, personalidad y delincuencia*, C.M. Romeo Casabona (Ed.), 2003, 159 pp.
- *Bases de datos, de perfiles de ADN y criminalidad*, C.M. Romeo Casabona (Ed.), 2002, 239 pp.
- Martin Uranga, Amelia, *La protección jurídica de las innovaciones Biotecnológicas: Especial consideración de su protección penal,* 2003, 547 pp.
- Urruela Mora, Asier*, Imputabilidad penal y anomalía o alteración psíquica*, 2003, 441 pp.
- *Principio de Precaución, Biotecnología y Derecho*, C.M Romeo Casabona (Ed.), 2004, 501 pp.
- Nicolás Jiménez, Pilar, *La protección jurídica de los datos genéticos de carácter personal,* 2006, 399 pp.
- Romeo Malanda, Sergio*, Intervenciones genéticas sobre el ser humano y Derecho Penal*, 2006, 426 pp.
- *Código de Leyes sobre Genética II, (Actualización 1997-2006),* 2007, 1110 pp.
- *Biotecnología, Desarrollo y Justicia,* C.M. Romeo Casabona (Ed.) 2008, 369 pp.
- De Miguel Beriain, Íñigo, *La clonación, diez años después*, 2008, 229 pp.
- *Retos de la investigación y comercialización de nuevos fármacos,* C.M. Romeo Casabona (Ed.), 2009, 227 pp.

- Jorqui Azofra, María, *Análisis genéticos en el ámbito asistencial: reflexión ético-jurídica,* 2010, 405 pp.
- *Los nuevos horizontes de la investigación genética,* C.M. Romeo Casabona (Ed.), 2011, 144 pp.
- *Más allá de la salud. Intervenciones de mejora en humanos*, C.M. Romeo Casabona (Ed.), 2012, 208 pp.
- *Hacia una nueva Medicina: consejo genético*, C.M. Romeo Casabona (Ed.), 2013, 255 pp.
- *Aspectos ético-jurídicos de las patentes biotecnológicas: la dimensión patrimonial de la materia viva,* C.M. Romeo Casabona (Ed.), 2014, 150 pp.
- *Bioterrorismo y bioseguridad,* C.M. Romeo Casabona (Ed.), 2015, 227 pp.
- *Tecnologías convergentes: Desafíos éticos y jurídicos,* C.M. Romeo Casabona (Ed.), 2016, 240 pp.

PUBLICACIONES PERIÓDICAS / PERIODICAL PUBLICATIONS

- Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada / Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine:
  Semestral desde 1994.

Revista de Derecho y Genoma Humano
Genética, Biotecnología y Medicina Avanzada

Law and the Human Genome Review
Genetics, Biotechnology and Advanced Medicine

Sumario

Summary

Número Extraordinario 2019 / Extraordinary Number 2019

Opinión / Opinion

Documento de información sobre la utilización de los datos de la historia clínica con fines de investigación biomédica en contextos de *big data*
Nuria Terribas i Sala (Coordinadora) Miembros del Proyecto de Investigación Bigdatius

Cuestionario/guía para la evaluación de proyectos de investigación con datos por un CEI (En cumplimiento del Reglamento Europeo 2016/679 de protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)
Iciar Alfonso Farnós / Guillermo Alcalde Bezhold / Miriam Méndez García

Doctrina / Articles

Nuevos desafíos en torno al *big data*
Gustavo Merino Gómez

Utilización de tecnología *big data* en investigación clínica
Guillermo Alcalde Bezhold / Iciar Alfonso Farnós

Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud
Carlos María Romeo Casabona

Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos
Pilar Nicolás Jiménez

Implicaciones jurídicas de la internacionalización de la tecnología del *big data* y derecho internacional privado
Alfonso Ortega Giménez

La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018
Miriam Méndez García / Iciar Alfonso Farnós

Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo
Inmaculada Vivas Tesón

Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías *big data*
Itziar Alkorta Idiakez

Pruebas genéticas en los tratamientos de reproducción asistida, con especial referencia a los tests de portadores y matching genético. Controversias en materia de información
Fernando Abellán-García Sánchez

Evaluación de proyectos de investigación con tecnología *big data* por un Comité de Ética de la investigación
Iciar Alfonso Farnós / Guillermo Alcalde Bezhold / Miriam Méndez García

Protección de los datos personales de salud en el proceso penal: efectos en la valoración de la prueba
Miren Josune Pérez Estrada

Transferencias internacionales de datos genéticos y datos de salud con fines de investigación
Mikel Recuero Linares

Informes / Reports

El derecho de los pacientes a sus *copyrights*
Virginia Díaz Gorriti / Rosa Mª Añel Rodríguez

IntimidAPP: Los problemas del tratamiento de datos biosanitarios en wearables y apps para móviles
Alberto Hidalgo Cerezo

Participative consent: Beyond broad and dynamic consent for health *big data* resources
María Villalobos-Quesada

La asistencia sanitaria transfronteriza a la luz del Reglamento General de Protección de Datos
Daniel Jove Villares

Tratamiento seguro de datos como factor de integración europea: implicaciones legales en el ámbito de la salud pública en Georgia
David Ruano Delgado / Nikoloz Phiphia

Una aproximación al *big data* y al blockchain sanitario y su implicación en la protección de datos personales
Lorena Pérez Campillo

Análisis doctrinal y jurisprudencial de los delitos de descubrimiento y revelación de secretos en el ámbito sanitario
Iker Conal Fuertes

Documentos / Documents

Informe 073667/2018 de la Agencia Española de Protección de Datos sobre la incidencia en el ámbito de la investigación biomédica del Reglamento General de Protección de Datos

The European Data Protection Board Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)

Bibliografía / Bibliography

Universidad del País Vasco / Euskal Herriko Unibertsitatea
NAZIOARTEKO BIKAINTASUN CAMPUSA
CAMPUS DE EXCELENCIA INTERNACIONAL
EUSKO JAURLARITZA GOBIERNO VASCO
HEZKUNTZA SAILA
DEPARTAMENTO DE EDUCACIÓN