UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

La Unión Europea como modelo de protección de datos en *eHealth*, su influencia y barreras a la convergencia

Alejandro Kress

Programa de Doctorado en Ingeniería de Proyectos y Sistemas

Escuela Técnica Superior de Ingeniería Industrial de Barcelona

Universitat Politècnica de Catalunya

Barcelona, enero 2017.

Tesis Doctoral

La Unión Europea como modelo de protección de datos en *eHealth*, su influencia y barreras a la convergencia

---

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Alejandro Kress

Bajo la dirección de

Prof. Dr. D. JOSEP MARÍA MONGUET FIERRO y

Prof. Dr. D. ENRIQUE NAVARRO CONTRERAS

Agradecimientos:

A mi madre, Dra. Marina Kress Voltz (farmacéutica, abogada y profesora de piano), gracias por haberme animado siempre a alcanzar la excelencia, como persona, en el plano académico y profesional. Y muy especialmente por encarnar el espíritu del esfuerzo, la perseverancia y la capacidad de superación, continuando con el espíritu de mi abuelo, Dr. Federico Kress Hohmann, superviviente de la batalla de Verdún (I Guerra Mundial), ahora que acaba de cumplirse precisamente el centenario de la misma.

A la familia Moreno Reyes, gracias por acompañarme en este apasionante camino de la vida, y a la familia Kress Trujillo, por un futuro lleno de buenos momentos compartidos.

Al Prof. Dr. Mª Monguet y Prof. Dr. Enrique Navarro, mis directores, por inspirar y guiar esta investigación pionera, donde se dan la mano la tecnología, el derecho y la salud.

Y a Don José Luis Blanco Ruíz, por su liderazgo, conocimientos y sabios consejos, todo un ejemplo a seguir para mí, así como a Don Javier Aparicio Salom, por su apoyo, valentía y tesón.

"La sociedad de la transparencia es la sociedad de la desconfianza, y de la necesidad del control, por eso la construcción de una sociedad de la transparencia es la asunción de la pérdida de valores esenciales como lealtad y honradez".

Han Byung-Chul
(1959-...)

ÍNDICE.

Resumen.

El 25 de mayo de 2018 se pone en práctica en la UE el Reglamento General de Protección de Datos, lo que representará un hito histórico, ahora que Europa sienta las bases legales del mercado único digital, que debe mejorar la calidad de vida de los europeos. En el entorno del *Big Data* en *eHealth* conviene evaluar la influencia de la actual regulación de la UE relativa a los datos de salud. Esta investigación surge de la idea de analizar la influencia del derecho a la protección de datos personales, nacido en Europa y proyectado en las últimas décadas en otras zonas geográficas como América Latina. La privacidad en el mundo del Big Data no está *per se* garantizada y es el propio ciudadano quién pide una protección común en la UE; este marco regulatorio de datos de salud se puede considerar un modelo de protección de datos en *eHealth* líder a escala internacional.

En 2016 se celebró el décimo aniversario del Día Internacional de la Protección de Datos, establecido a iniciativa del Comité de Ministros del Consejo de Europa y la Comisión Europea para concienciar a todos los ciudadanos. Vivimos tiempos de innovación y competitividad, donde los datos de salud están muy cotizados, pero queda un camino por recorrer para superar los riesgos en este campo. Las ciencias de la vida y las nuevas tecnologías están produciendo una enorme cantidad de datos que son la base de nuevos descubrimientos científicos, necesarios para la mejora de nuestra la salud y calidad de vida. Para contribuir a estos avances en la ciencia, se despliegan múltiples bases de datos y herramientas, con sistemas que son variados y complejos técnicamente, aplicados a diferentes disciplinas científicas. El uso de estos recursos, diversos y fragmentados en muchas ocasiones, ha conducido a la UE a desarrollar distintas iniciativas para la normalización del acceso y el tratamiento de la información y los sistemas, dando lugar a lo que podemos calificar como un modelo de referencia. Esta investigación pretende arrojar luz en cuanto al motor de este modelo y sus implicaciones fuera del territorio europeo, especialmente teniendo en consideración la experiencia en América Latina, debido a sus vínculos culturales, lingüísticos y de cooperación comercial con España.

Se trata de valorar la magnitud que hoy tienen conceptos como Big Data, *eHealth*, protección de datos e historia clínica electrónica, después de casi 50 años de avances en materia de protección de datos, desde que, en el seno de Europa, apareció la primera regulación de protección de datos de carácter personal. La Unión Europea es la jusrisdicción más regulada en materia de protección de datos y son los propios ciudadanos europeos los que han impulsado los cambios legislativos y la defensa de sus derechos. La ley protege un derecho fundamental como es la protección de datos de carácter personal, y de forma especial los datos de salud, considerados datos sensibles y por lo tanto especialmente protegidos. La investigación científica y la atención sanitaria en el entorno de *eHealth* también requieren un marco de trabajo estable, con seguridad jurídica, en el que ha trabajado la Comisión Europea. El artículo 4 de la Ley Orgánica 15/1999

(que en España traspone la Directiva 95/46/CE de protección de datos de carácter personal) en su apartado 1 estipula que “Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”. En general, la transmisión de datos de salud a terceros se considera una cesión de datos, es decir, una revelación de datos realizada a una persona distinta del propio interesado, y como establece el artículo 7.3 de la Ley Orgánica 15/1999 “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”, aunque el artículo 11.2 f) de la misma Ley señala que el consentimiento exigido en el apartado anterior no será necesario...”cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica”. Esta Ley Orgánica 15/1999 y demás legislaciones de los Estados miembros relativas a la protección de datos continúan en vigor hasta su modificación, aunque ajustadas a los criterios que establece el nuevo Reglamento (UE) 2016/679, que incluye novedades como un endurecimiento del régimen sancionador.

Los datos de salud, como consumidores y usuarios, conllevan enormes problemas relativos a la privacidad y la seguridad. Por ello la política sobre privacidad se presenta como una materia que va a desempeñar un papel estratégico especialmente en las empresas que traten datos de ciudadanos europeos. La especial protección que reciben los datos de salud en Europa marca tendencia a la vez que la UE se erige como modelo internacional de protección de datos.

Palabras clave.

Metadatos, salud digital, atención sanitaria, protección de datos, Unión Europea, América Latina, derecho a la privacidad, Internet, redes sociales.

Abstract.

The General Data Protection Regulation at EU level to be implemented 25 May 2018 will represent an historic achievement at a time when the Europe is laying the foundations of a digital single market, that shall improve the quality of life of Europeans. In the context of Big Data and *eHealth*, it is convenient to tackle the influence of the current EU regulation related to health data. This research was conceived from the idea of assessing the influence of the right to personal data protection, born in Europe and projected in the last decades in other regions such as Latin America. Privacy and data protection in the era of Big Data are not *per se* guaranteed. It is the citizens themselves who are asking for a harmonized protection within the EU; this health data regulatory framework can be regarded as a leading data protection model in *eHealth* internationally.

2016 represented the 10th anniversary of the International Data Protection Day, a celebration that was established by the committee of ministers of the Council of Europe and the European Commission to raise awareness amongst citizens. We are living a time of innovation and competitivity, where health date are highly valuable, but substantial progress needs still to be made to overcome the risks this matter triggers. Life sciences and new technologies are producing a vast amount of data that are the basis of new scientific findings (amongst many other potential uses) that help to improve our health condition and quality of life. In order to contribute to this scientific progress, an undetermined number of databases and tools are deployed, with a varied and technically complex set of systems applied to several scientific disciplines. The use of these resources, diverse and fragmented in many cases, has led the EU to develop a number of initiatives to standardize the accesss and management of both information and systems, representing what I call a benchmark model. This research aims at shedding light on the engine of this model and its implications beyond Europe, looking at Latin America, based on the cultural, linguistic and commercial cooperation links with Spain.

It is about assessing the current magnitude of concepts such as Big Data, *eHealth*, data protection and electronic health records, after 50 years of progress in the area of data protection, when in the heart of Europe, the first regulation of personal data protection was born. The European Union is the most regulated jurisdiction when it comes to data protection, and it is the European citizens themselves who have promoted legal changes and the defence of their rights. The law protects a fundamental right such as the protection of personal data, and especially health data, regarded as sensitive data, and therefore especially protected. Scientific research and healthcare in the *eHealth* environment require a stable framework, with legal certainty, in which the European Commission has been working extensively. Article 4 of the Organic Law 15/1999 (which in Spain transposes Directive 95/46/EC on the protection of personal data), paragraph 1, reads “Personal data may only be collected for processing and processed where appropriate, pertinent and

not excessive in relation to scope and the specific, explicit and legitimate purpose for which they were obtained". Overall, the transmission of health data to third parties is regarded as a data transfer, that is, a disclosure of data made to a person other than the concerned person, and as established in article 7.3 of Organic Law 15/1999 "personal data that refer to racial origin, health and sexual life may only be collected, treated and transferred when, for reasons of general interest, approved by the Law or with express consent of the person concerned", although article 11.2 f) of the same Law states that "the consent required in the previous section will not be required...when the transfer of personal data related to health be necessary to solve an emergency that requires access to a file or to conduct epidemiological studies in the terms established in the legislation on national or regional healthcare". This Organic Law 15/1999 and all other data protection laws of member States remain in force until their amendment, although adjusted to the new criteria established by the Regulation (EU) 2016/679, that includes tightened sanctions.

Healthcare data trigger colossal privacy and security issues, therefore the privacy policy appears to play a pivotal role within the future strategy of the businesses dealing with data of European citizens. The special protection that health data receive in Europe is trendsetting while the EU emerges as a model of global data protection regime.

Keywords.

Big Data, *eHealth*, healthcare, data protection, healthcare, European Union, Latin America, privacy law, Internet, social networks.

LISTADO DE FIGURAS

LISTADO DE TABLAS

LISTADO DE GRÁFICOS

LISTADO DE ABREVIATURAS y ACRÓNIMOS

AEPD: Agencia Española de Protección de Datos.

BOE: Boletín Oficial del Estado.

CE: Constitución Española.

CEDH: Convenio Europeo de Derechos Humanos.

CGPJ: Consejo General del Poder Judicial LOPD Ley Orgánica de Protección de Datos.

CPOE: Computerized Physician Order Entry.

DPO: Data Protection Officer.

ECHR: European Convention of Human Rights.

EE.UU.: Estados Unidos de América.

EHR: Electronic Health Record.

EMR: Electronic Medical Record.

ENCR: European Network of Cancer Registries.

EORTC: European Organisation for Research and Treatment of Cancer.

ETSI: European Telecomunications Standard Institute.

EUPATI: Academia Europea de Pacientes.

FRA: European Union Agency for Fundamental Rights.

HIPAA: Health Insurance & Portability and Accountability Act.

HMO: Health Maintenance Organization.

IEC: International Electrotechnical Commission.

IoT: Internet of Things / Internet de las Cosas.

ISMS: International information security management system.

ISO: International Standardization Organization / Organización Internacional de la Normalización.

HCE: Historia Clínica Electrónica.

HIS: Health Information System.

LOPD: Ley Orgánica 15/1999, de Protección de Datos Personales, de 13 de diciembre.

LORTAD: Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

M2M: Machine to Machine.

NSA: National Security Agency.

OMS: Organización Mundial de la Salud.

ONU: Organización de Naciones Unidas.

PDAs: Asistentes personales digitales.

RGPD: Registro General de Protección de Datos.

RLOPD: 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.

SNS: Social Networking Sites.

TC: Technical Committee / Comité Técnico.

TI: Tecnología de la información.

TIC: Tecnologías de la información y la comunicación.

TJCE: Tribunal de Justicia de las Comunidades Europeas.

TJUE: Tribunal de Justicia de la Unión Europea.

UE: Unión Europea.

UNESCO: United Nations Educational Scientific and Cultural Organization.

Introducción.

Con la llegada del Big Data[1] estamos viviendo la **génesis de la competitividad**, como lo definen McAfee[2] y Brynjolfsson[3] (2012), que unos años antes (McAfee y Brynjolfsson, 2008) ya titularon su artículo en Harvard Business Review *"investing in the IT that makes a competitive difference"*; pero apuntan muy acertadamente que "no es oro todo lo que reluce" (si se me permite la expresión), sino que se más bien se trata de convertir el Big Data en oro competitivo. El Big Data puede ser la **génesis de todo lo que es tendencia**, la génesis de los negocios, pero se trata de unos datos que provienen de múltiples fuentes, y aparecen en distintos formatos, a menudo profundamente desestructurados (Copping y Li, 2016).

Nadie duda de los beneficios de las TIC pero el riesgo potencial asociado al Big Data ha motivado un intenso debate a lo largo de los últimos años, a la vez que la Unión Europea ha trabajado de forma constante durante varios años en un nuevo marco regulatorio de protección de datos, que tendrá una derivada directa para todas las organizaciones que trabajan el Big Data (incluidas las firmas de almacenamiento de datos); el tratamiento de la información debe ajustarse a prácticas lícitas y acordes con los derechos de las personas, pues son los legítimos titulares de la información; **el individuo, motor de la innovación**, cobra personalidad propia a la vez que utiliza todos los nuevos recursos a su alcance como las redes sociales y las webs especializadas que contribuyen a la explosión del Big Data.

Los ciudadanos europeos, a pesar de sus diferencias culturales y de las diversas actitudes individuales frente a la privacidad, piden una armonización de la protección de la información personal. Se analiza en esta investigación la situación en España y resto de Europa sobre cultura de protección de datos; la cooperación de las instituciones médicas y de salud, que reciben un 74% (2015)[4]/78% (2011)[5] de apoyo de la población de la UE[6], parece que pueden y deben liderar, junto a las instituciones europeas, la transición

[1] Ver apartado 2.1. que aborda este concepto en profundidad.

[2] Andrew Paul McAfee es co-director del MIT Initiative on the Digital Economy y director asociado del Center for Digital Business del MIT Sloan School of Management, estudioso de cómo la tecnología de la información afecta a las empresas (http://andrewmcafee.org. Último acceso 3 enero 2017).

[3] Erik Brynjolfsson es the co-Director del MIT Initiative on the Digital Economy y profesor del MIT Sloan School, y presidente del MIT Sloan Management Review, estudioso de los efectos de la tecnología de la información en la estrategia de los negocios, la productividad y el rendimiento, el comercio digital y los bienes intangibles (http://mitsloan.mit.edu/faculty-and-research/faculty-directory/detail/?id=22672. Último acceso 3 enero 2017).

[4] Dato de la Comisión Europea. Eurobarómetro especial 431 (2015), con 28 Estados miembros.

[5] Dato de la Comisión Europea. Eurobarómetro especial 359 (2011), con 27 Estados miembros.

[6] La Europa de los 28 tras la incorporación de Croacia el 1 de julio de 2013 parte por un conjunto de países que firmaron los Tratados que conforman la UE; Los Tratados constitutivos de la Comunidad Europea del Carbón y el Acero, la Comunidad Económica Europea y la Comunidad Europea de la Energía Atómica. Existen otros Tratados de reforma puntual de los Tratados constitutivos, como la Convención de Roma del 1957 o los Tratados de Bruselas de 1965, 1975 y 1984 y de Luxemburgo de 1970; Tratados de reforma sustancial, como son el Acta Única y el Tratado de la Unión Europea, el Tratado de Ámsterdam y el Tratado de Niza. Posteriormente llegan los Tratados de adhesión de Dinamarca, Irlanda y Reino Unido que entraron en vigor el 1 de enero de 1973. La segunda ampliación llegó con la entrada de Grecia en la comunidad, el 1 de enero de 1981, tras la caída del régimen militar. Más tartde fue el turno de España y Portugal, su adhesión se produjo el 12 de junio de 1985, entrando en vigor el 1 de enero de 1986. Con la adhesión de Finlandia, Austria y Suecia, el 1 de enero de 1995, la Unión Europea se convierte en la Europa de los quince. La quinta ampliación trae

hacia un *eHealth* eficiente, a través de la interoperabilidad entre los sistemas de distintos países.

Los Estados miembros de la UE han implementado la Directiva de 1995 relativa a la protección de datos de forma diferente, pero a pesar de ello parece razonable concluir que una mayoría de los ciudadanos europeos confían en que se producirá una convergencia de las políticas de protección de datos[7]; la nueva regulación europea en la materia debería eliminar las divergencias y costes asociados para las empresas, pudiendo convertirse el modelo a seguir como política líder a nivel global; uno de los grandes proyectos de la UE en materia sanitaria es la accesibilidad de los datos a través de la historia clínica electrónica (en adelante, HCE); en 2012 la Comisión Europea propuso una reforma para armonizar cómo se recogen los datos, su acceso y su uso; el Reglamento (UE) 2016/679 incluye novedades como el endurecimiento del régimen sancionador y la figura del delegado de protección de datos, todo ello con enorme relevancia para el futuro de la privacidad (Martínez, 2016), a la vez que se pretende impulsar la economía digital y la innovación. Por primera vez en 20 años se va a sustituir la actual normativa[8], lo que va a representar el paso de una regulación vía directiva (que exige la consiguiente transposición al ordenamiento de cada Estado miembro) a una regulación vía reglamento (directamente aplicable en los Estados miembros)[9].

Es cada día mayor el movimiento de ciudadanos por razones de trabajo, por estudios, por vacaciones, etcétera...es decir, de pacientes, y de profesionales de la salud; unos buscan y otros ofrecen asistencia sanitaria en una Unión Europea con más miembros y en un mundo globalizado. Esta realidad impone una mejor la coordinación de políticas y sistemas de salud en toda la UE; se trata de dar respuesta a las cuestiones relacionadas con la **asistencia sanitaria transfronteriza** en Europa[10], materia que está ligada

---

la adhesión de diez nuevos miembros: Polonia, Republica Checa, Eslovaquia, Hungría, Eslovenia, y los Estados Bálticos de Estonia, Letonia, Lituania, más Chipre y Malta. La penúltima ampliación convierte a Rumania y Bulgaria (el 1 de enero de 2007) en miembros de la UE, y la misma pasa a estar formada por 27 Estados miembros, antes de la incorporación de Croacia (Representación de España ante la UE. Recuperado de http://www.exteriores.gob.es/RepresentacionesPermanentes/EspanaUE/es/quees2/Paginas/El-Derecho-comunitario.aspx. Último acceso el 30 diciembre de 2016).

[7] Comisión Europea, Eurobarómetro especial 359, 2011.

[8] En este contexto conviene señalar que el Derecho comunitario es el Ordenamiento Jurídico propio proveniente de las instituciones comunitarias, que se integra en los sistemas jurídicos de los Estados miembros y se impone a sus órganos jurisdiccionales, tiene primacía sobre el derecho nacional para así garantizar su uniformidad en todos los Estados miembros, y además tiene autonomía con respecto al Derecho interno de los Estados. Esta integrado por el Derecho originario y por el Derecho derivado. El Derecho originario actúa como norma fundamental o constitucional de la Unión Europea, se integra por un conjunto de Tratados. El Derecho derivado consiste en el conjunto de normas y actos comunitarios emanados de las instituciones de la Unión Europea, en virtud de las habilitaciones genéricas o especificas del Derecho originario, como son reglamentos, directivas y decisiones (Representación de España ante la UE. Recuperado de http://www.exteriores.gob.es/RepresentacionesPermanentes/EspanaUE/es/quees2/Paginas/El-Derecho-comunitario.aspx. Último acceso el 30 diciembre de 2016).

[9] Las directivas deber ser incorporadas al ordenamiento de los Estados miembros destinatarios en los plazos fijados en las mismas. El TJCE rechaza alegaciones de los gobiernos argumentando problemáticas de índole interno para dilatar o impedir su cumplimiento; tampoco acepta argumentaciones basadas en la complejidad de las modificaciones legislativas requeridas.

[10] Torres (2016) en relación con la asistencia sanitaria en el marco europeo se refiere a las diferentes normativas aplicables en los siguientes términos: "Los ciudadanos europeos pueden hacer uso de la asistencia sanitaria en UE pudiendo regirse por distinta normativa. Una forma de acceder o vía de acceso al uso de la asistencia sanitaria europea son las normas sobre Coordinación de la Seguridad Social que no reemplazan los regímenes nacionales por un régimen europeo único, sino que cada país sigue siendo libre de decidir, según su propia legislación, quién está asegurado, que prestaciones percibe y qué requisitos debe cumplir. La Jurisprudencia del TJUE ha jugado un papel importante para ampliar la cobertura y prestaciones de asistencia sanitaria que reciben los ciudadanos europeos, y es otra forma de acceso a la asistencia sanitaria en la UE. Otra vía, forma o procedimiento que los ciudadanos europeos tienen para acceder a la asistencia sanitaria en la UE es 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. Esta Directiva

a la movilidad de los pacientes, con implicaciones financieras, atendiendo al control de la calidad, a los derechos de los pacientes[11]; la historia de la movilidad de los pacientes en Europa se remonta a cuando los ciudadanos cruzaban las fronteras; ya en la Edad Media, los peregrinos que necesitaban cuidados podían confiar en una red de monasterios que ofrecían atención gratuita, aunque básica, mientras avanzaban lentamente hacia centros urbanos como Santiago de Compostela. La situación actualmente es, con gran diferencia desde luego, muy diferente. Por una lado los ciudadanos y viajeros atraviesan de un país a otro de la UE sin fronteras o aduanas, y no a caballo, sino que transportados en trenes, automóviles y otros medios de trasnporte modernos, incluido el avión. Por otro lado, la atención sanitaria puedo hoy en día ofrecer productos farmacéuticos y tecnologías más sofisticados, lo que facilita no sólo el tratamiento de enfermedades, sino que mejora la calidad de vida, y hasta prolongan la vida misma. Sin embargo, hasta que la UE ha establecido mecanismos para la asistencia sanitaria transfronteriza, se trataba de una cuestión meramente privada si algun ciudadano precisaba asistencia sanitaria en otro país comunitario, de la misma forma que hoy muchos viajeros que precisan de atención médica más allá de su país realizan el desembolso correspondiente que luego reclaman a través de su póliza de seguro de viajes[12].

Fue en los primeros años de la década de 1970-1980 cuando la entonces Comunidad Económica Europea pasó a reconocer que el principio de la libre circulación de personas, uno de los cuatro pilares consagrados por los Tratados europeos, carecía de sentido que sólo fuera aplicable a aquellos ciudadanos que gozaban de buena salud; el 14 de junio de 1971 se aprobó el Reglamento nº 1408/71 del Consejo, relativo a la aplicación de los regímenes de seguridad social a los trabajadores por cuenta ajena, a los trabajadores por cuenta propia y a los miembros de sus familias que se desplazaran dentro de la Comunidad[13]; se establecían una serie de mecanismos mediante los cuales las personas podían obtener asistencia sanitaria en otro Estado miembro.

La situación sufrió una transformación muy seria en 1998, con dos sentencias vinculadas del Tribunal de Justicia de las Comunidades Europeas en los casos Kohll y Decker, referidos a pacientes que podían utilizar las disposiciones del mercado interior para acceder a la asistencia sanitaria en otros Estados miembros; la Comisión Europea convocó un proceso de reflexión de alto nivel para abordar explícitamente la cuestión de la **movilidad de los pacientes**. Este proceso de reflexión condujo a una serie de recomendaciones que buscaban maximizar los beneficios potenciales de la movilidad de los pacientes, minimizando al mismo tiempo los problemas.

---

ha sido transpuesta en nuestro ordenamiento jurídico español a través del Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza; ambas conforman la otra vía de acceso a la asistencia sanitaria en la UE".

[11] De acuerdo con el informe de política basado en los debates de un seminario internacional organizado por la Comisión Europea, el Gobierno Regional de Veneto, el Ministerio italiano de Salud y el Observatorio (Venecia, 26-27 de octubre de 2005).

[12] Contenido del informe *Cross Border Heatlh Care in Europe* del European Observatory on Health Systems and Policies. Recuperado de http://www.euro.who.int/__data/assets/pdf_file/0006/108960/E87922.pdf. Último acceso 6 diciembre de 2016

[13] Versión consolidada publicada en el Diario Oficial de las Comunidades Europeas n ° L 28 de 30.1.1997.

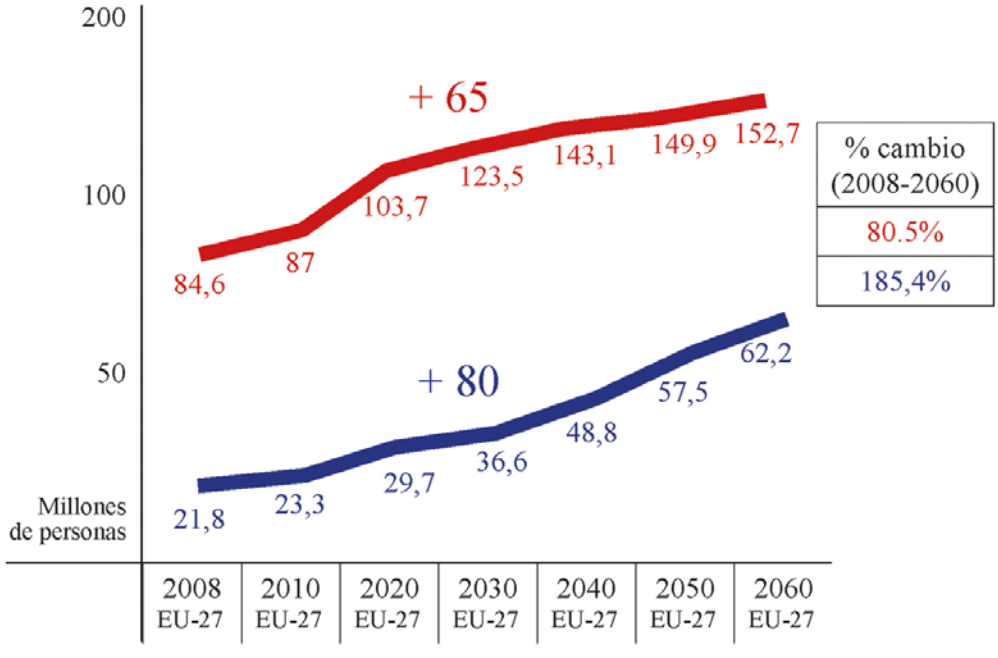
La movilidad de pacientes y profesionales dentro de la Unión Europea nos lleva a plantearnos preguntas complejas sobre su impacto, con especial atención a los datos de salud. Hoy en día, los pacientes viajan y caen enfermos en sus desplazamientos, o viajan precisamente para recibir tratamiento otros países distintos al suyo propio de residencia, y a veces buscan tratamientos que se encuentran al margen de las coberturas financiadas por su sistema público de salud; como pueden ser operaciones de cirugía estética o tratamientos dentales. Pero también están los casos de los inmigrantes en situación "administrativa irregular" (Lema Tomé, 2014); se trata de personas procedentes de fuera de la UE, muchas de las cuales no gozan del derecho a la asistencia sanitaria en su país de residencia y, por esta razón no tendrán derecho a ser reconocidos de forma generalizada por otros Estados miembros de la UE.

Por otro lado, en la coyuntura actual nos encontramos con sistemas de salud, dentro y fuera de la UE, donde reina el envejecimiento demográfico de la población (Dixon y Scheurell, 2016; Adamson, 2016; Kankanhalli, Hahn, Tan y Gao, 2016; Suzman, Beard, Boerma y Chatterji, 2015), lo que incrementa el gasto público al crecer la proporción de la población que recibe pensiones públicas y servicios de salud (Clements, Dybczak y Soto, 2016; Adamson, 2016). Sistemas de salud que están experimentando además la aplicación de nuevas tecnologías (González, Pascual y Mora, 2016; Pratt y Franklin, 2016; Wildman, McMeekin, Grieve y Briggs, 2016; Cresswell, Bates y Sheikh, 2016; Cresswell, Coleman, Smith, Swainson, Slee y Sheikh, 2016; Percival y McGregor, 2016; Ranallo, Kilbourne, Whatley y Pincus, 2016; Zalon, 2016; Garavand, 2016; Nielsen y Sæbø 2016; Williams, 2016; Janssen, 2016), y técnicas sanitarias (Regmi, Bendel y Gee, 2016; Adamson, 2016; Köppe, 2016; Moore, Persaud y Torchia, 2015; Beidas, 2015).

Con todo ello, la salud es uno de los sectores que mayor gasto representa para muchos gobiernos de todo el mundo (Palladino, Lee, Hone, Filippidis y Millett, 2016; Martin, Hartman, Benson, Catlin y National Health Expenditure Accounts Team, 2016); con el envejecimiento de la población, el aumento de las expectativas de vida y el desarrollo de tratamientos innovadores de salud, el gasto va en aumento, como señala Adamson (2016). El incremento del gasto en sanidad es una de las principales preocupaciones para los gobiernos, y especialmente para la UE y sus Estados miembros, que se han visto obligados a imponer medidas para recortar los gastos (Rich y Merrick, 2006), e incluso a **derivar parte de los costes a los propios pacientes** (Meyer, 2016; Denmark, 2016), a raíz también de las medidas de austeridad impuestas por muchos gobiernos a raíz de las crisis financiera mundial de 2008 (Labonté y Stuckler, 2016), lo que ha impulsado el uso de las TIC en el sector sanitario, debido a las ventajas que ofrecen para maximizar la calidad y la eficiencia (Shoniregun, Dube y Mtenzi, 2010). La Comisión Europea juega un papel fundamental a la hora de perseguir la estabilidad política y económica en la Unión Europea, y contribuir al desarrollo de las innovaciones médicas y tecnológicas, muchos de los esfuerzos actuales de la Comisión Europea ya se dirigen a fortalecer los sistemas de salud; como recuerda Janssen (2016) se prevé que el

número de personas de 65 o más años de edad en el año 2060 (en toda la UE excluyendo Croacia) aumentará en un 80,5% (en una proyección desde 2008), a la vez que se estima que el número de personas de 80 o más años de edad casi llegará a triplicarse durante ese mismo período (ver gráfico 0.0.).

Gráfico 0.0.
Proyecciones sobre envejecimiento de la población, en millones de personas, mayores de 65 años y de 80 años en la UE (excluida Croacia), 2008-2060.

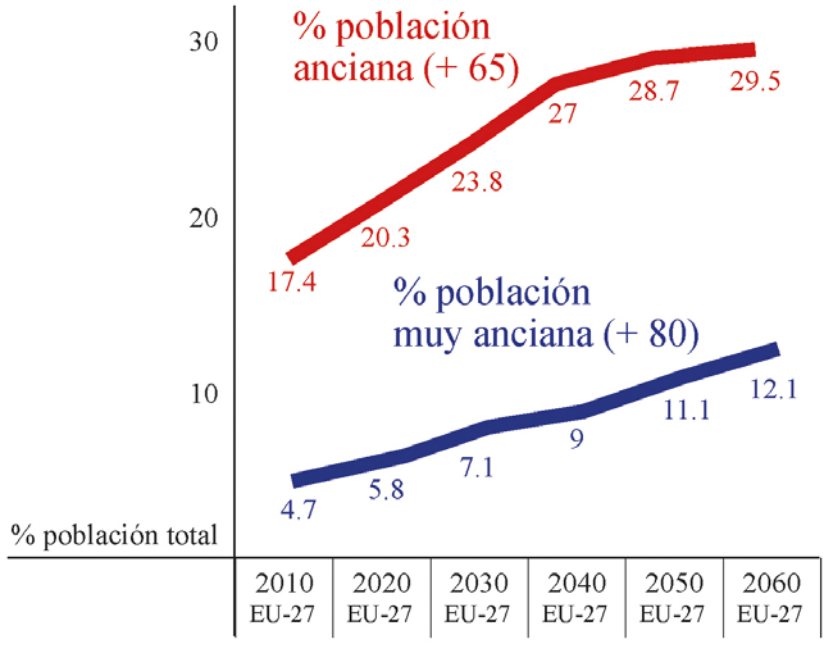


Fuente: gráfico de elaboración propia a partir del Informe de Envejecimiento 2012 de la Comisión Europea.

El 12 de mayo de 2015 se emitieron las conclusiones del Consejo de la UE sobre la sostenibilidad de las finanzas públicas ante el envejecimiento de la población[14], según las cuales se prevé que el gasto público en atención sanitaria y en cuidados de larga duración aumente en la UE en 2 puntos porcentuales del PIB entre 2013 y 2060, con diferencias significativas por país, hasta llegar a alcanzar el 10,6 % del PIB en 2060, por razón de la evolución demográfica fundamentalmente. Teniendo en cuenta la evolución actual, se prevé que el aumento previsto del gasto en atención sanitaria y cuidados podría incluso llegar a 4 puntos porcentuales del PIB entre 2013 y 2060. En el siguiente gráfico 0.1. se puede comprobar cuáles son las proyecciones de envejecimiento de la población en la UE (excluida Croacia) desde el 2010 hasta el año 2060, expresado como porcentaje de la población total.

[14] Consejo de la UE. Conclusiones del Consejo sobre la sostenibilidad de las finanzas públicas ante el envejecimiento de la población. Recuperado de http://www.consilium.europa.eu/es/press/press-releases/2015/05/12-ecofin-ageing-populations/. Último acceso el 12 de noviembre de 2016.

Gráfico 0.1.
Proyecciones demográficas de la población de ancianos en la UE, 2010-2060.



Fuente: gráfico de elaboración propia a partir del Informe de Envejecimiento 2012 de la Comisión Europea.

Los ciudadanos europeos gozan de una vida más sana y duradera, su esperanza de vida es cada vez mayor, a un ritmo de 2 a 3 meses cada año[15]. Las razones principales de este crecimiento de la esperanza de vida son los estilos de vida -más saludables-, los niveles de vida -más altos-, la educación -de mejor calidad- y el acceso a servicios de salud de calidad -más fácil- (Mathers, Stevens, Boerma, White y Tobias, 2015; Organización para la Cooperación y el Desarrollo Económico, 2011).

En este contexto, donde todos los países de Europa están experimentando un envejecimiento de sus poblaciones[16] y con menos personas en edad de trabajar por jubilados (Rechel, Doyle, Grundy y Mckee, 2009), la EU está apoyando el desarrollo del *eHealth*, con la implementación de la nuevas tecnologías en el sector sanitario, para reducir costes[17] y mejorar la eficiencia del servicio (Van Rooij y Marsh, 2016).

[15] Social Protection Committee (2014). Adequate social protection for long-term care needs in an ageing society. Recuperado de http://ec.europa.eu/health/ageing/docs/ev_20140618_co04_en.pdf. Último acceso 6 Diciembre 2016.

[16] Precisamente en un contexto internacional donde se prevé que la población mundial alcanzó 7.200 millones en 2014, y se espera que para 2050 habrá aumentado más de 2.000 millones, donde precisamente la mayor parte del crecimiento de la población tendrá lugar en las regiones menos desarrolladas; se estima que la población de África y de Asia aumentará en gran medida (por encima de Europa) en las próximas décadas (Naciones Unidas, 2014. La situación demográfica en el mundo, 2014. Informe Conciso. Departamento de Asuntos Económicos y Sociales. División de Población. Nueva York).

[17] Al margen del envejecimiento de la población, hay que tener en cuenta el aumento de los costes motivado por los flujos migratorios en la UE y alrededor del mundo, que han creciendo de forma exponencial y hoy en día una de cada siete personas en el mundo es migrante, según el informe de de la Organización Internacional de las Migraciones (2014); un aspecto adicional relevante que se añade al aumento de los movimientos migratorios son las direcciones de las migraciones, que tradicionalmente han situado como lugares de recepción a los polos de desarrollo económico (la UE entre

El Reglamento (UE) 2016/679 de protección de datos, a aplicar desde 25 de mayo de 2018, representará un nuevo hito histórico, mientras en Europa se sientan las bases legales del **mercado único digital**[18]; esta nueva regulación que exigirá una profunda aclaración por parte de autoridades y jurisprudencia, abriendo nuevas necesidades de especialistas como los delegados de protección de datos (Hernández, 2016). La Comisión Europea tiene por objetivo la creación de un mercado único digital para que consumidores y empresas puedan beneficiarse de un **espacio económico de más de 27 países y 500 millones de personas**, superando todo tipo de barreras, desde las tecnológicas a las legales o fiscales (Castaneda, 2016). Así, por ejemplo, la Agenda Digital -parte integrante de la estrategia Europa 2020[19]- prevé que la robótica (acompañada de la inteligencia artifical) mejorará la competitividad industrial de la UE por medio de las tecnologías, dispositivos y servicios que deben contribuir a ofrecer remedios para los retos a los que se enfrenta Europa, como el **envejecimiento de la población**. La investigación y la innovación digitales del mercado único deben impulsar, de acuerdo con la Agenda Digital de la UE, la futura prosperidad y calidad de vida europeas.

El 6 de mayo de 2015 la Comisión Europea presentó su estrategia para el mercado único digital; recogida en un documento donde la Comisión introduce un conjunto de acciones para alcanzar un mercado donde la libre circulación de mercancías, personas, servicios y capitales quede garantizada, y donde se facilite a personas y empresas acceder con facilidad a sus actividades, y ejercerlas en red (conectados) en condiciones de competencia, **con un elevado nivel de protección de datos personales y de consumidores**, sin importar su nacionalidad o lugar de residencia (Zárraga, 2015). El 15 de febrero de 2013 ya había aprobado el Consejo de Ministros la Agenda Digital para España como la estrategia del Gobierno español para desarrollar la economía y la sociedad digital a escala nacional, con seis principales objetivos[20]: (1) fomentar el despliegue de redes y servicios para garantizar la conectividad digital (2) desarrollar la economía digital para el crecimiento, la competitividad y la internacionalización de la empresa (3) mejorar la administración electrónica y los servicios públicos digitales (4) reforzar la confianza en el conexto digital (5) impulsar I+D+I en las industrial del futuro y (6) promover la alfabetización digital y la formación de profesionales TIC.

---

otros), y como lugares de emisión a los polos considerados en vía de desarrollo o zonas de pobreza; es decir, migraciones tradicionalmente entendidas como provenientes del sur, con puntos de llegada en el norte (Novella, 2015).

[18] La Agenda Digital para Europa se creó en mayo de 2010 para impulsar la economía europea aprovechando las ventajas económicas y sociales sostenibles del mercado único digital.

[19] Comisión Europea. Europa 2020. Recuperado de http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_es.htm. Último acceso 2 enero 2017.

[20] Agenda Digital para España. Recuperado de http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx. Último acceso 5 enero 2017.

Internet y la tecnología digital está transformando nuestro mundo, pero las barreras existentes *online* hacen que los ciudadanos pierdan bienes y servicios. Las empresas de Internet y las empresas de nueva creación *(starts-up)* tienen un horizonte limitado, pues las empresas y los gobiernos no pueden beneficiarse plenamente de las herramientas digitales. Es por ello de que lograr que el mercado único de la UE encaje en la era digital, derribando los muros reguladores y pasando de un mercado fragmentado a un mercado único que podría contribuir con 415.000 millones de euros al año a la economía comunitaria y crear cientos de miles de nuevos puestos de trabajo[21].

Esta investigación aborda el alcance de la política de protección de datos de la UE en un contexto internacional, con atención a la región latinoamericana, especialmente en relación a los datos personales masivos (denominados en esta investigación como "Big Data", y definidos en el apartado 2.1.1.) en el ámbito de la salud digital (denominada en adelante "*eHealth*" y definida en el apartado 2.1.2.).

Se acaba de celebrar en 2016 el décimo aniversario del Día Internacional de la Protección de Datos, establecido a iniciativa del Comité de Ministros del Consejo de Europa y la Comisión Europea para concienciar a los ciudadanos sobre la importancia de proteger su privacidad. Los datos de salud están muy cotizados, pero su uso conlleva riesgos. Por ello la política de privacidad se presenta como una materia que va a desempeñar un papel estratégico especialmente en las empresas que tratan datos de ciudadanos europeos, a la vez que la UE parece eregirse como modelo internacional de protección de datos.

Mañas (2009) abarca la temática de seguridad, transparencia y protección de datos en un futuro, ya presente, con un necesario e incierto equilibrio: "se trata de reconocer que la sociedad actual está sometida a amenazas hasta ahora no conocidas, que tienen mucho que ver con el uso de nuevas y sofisticadas tecnologías, y que permiten a muy bajo costo generar riesgos reales para la seguridad ciudadana".

Álvarez Hernando (2011) en su guía práctica sobre protección de datos incluye las cuestiones más relevantes en materia de protección de datos, con comentarios de las resoluciones de la Agencia Española de Protección de Datos, además de sentencias destacadas; se puede decir que hoy existe un más fácil acceso, por parte de los ciudadanos, a documentos de seguridad, cláusulas legales, modelos de ejercicio de derechos de acceso, rectificación, cancelación u oposición, etcétera...que afecta en general a todos los responsables del cumplimiento de la normativa de protección de datos en empresas y organismos púlicos y privadas. En este sentido como señala Álvarez Hernando hay que prestar una especial atención a ámbitos donde el tratamiento de datos es especialmente relevante, como es el caso de los ficheros de morosos, además de otros temas de

[21] Tal y cómo recoge la propia Comisión Europea. Marché Unique Numérique. Recuperado de http://ec.europa.eu/priorities/digital-single-market/index_fr.htm. Último acceso 1 diciembre 2016.

actualidad como la video-vigilancia, los tratamientos de datos realizados por parte de abogados y procuradores, comunidades de propietarios...Administración Pública en general, includos los **centros de salud** en particular. Existen tratamientos de datos en infinidad de ámbitos como las relaciones laborales, Internet, la publicidad y todo lo relacionado con la prospección comercial, a través bien de medios tradicionales o bien de las nuevas tecnologías de la información.

Ahora que llega un nuevo marco regulatorio, el Reglamento General de Protección de Datos, Mañas, Caro y Gayo (2016) se plantean cómo va a convivir con la vigente legislación. A este respecto Piñar Mañas se posiciona a favor de que la normativa nacional derivada de la Directiva 95/46/CE, como es la LOPD, podrá seguir siendo aplicable en aquel ámbito que esté fuera de la materia regulada en el RGPD, ya que entiende que el RGPD hace numerosas remisiones a la legislación nacional de los Estados miembros, aunque el papel de la AEPD debe ser revisado en este nuevo contexto.

Antecedentes.

Europa ha sido pionera en la protección de datos. El modelo europeo se impone como líder en la defensa de una estricta protección de la privacidad a favor de los individuos[22]. La Convención Europea de Derechos Humanos[23] ratificada en 1953 representa el primer tratado internacional que protege derechos humanos en Europa y en concreto atiende a "la protección de derechos fundamentales a la luz de los cambios y desarrollos tecnológicos"; todos los países de la UE son firmantes de dicho tratado.

Varias Constituciones Europeas recogen el derecho a la privacidad[24], relacionado directamente, (según Gregorio, 2004) con las experiencias de la Segunda Guerra Mundial, los archivos del gobierno y datos del censo de judíos y otras víctimas de genocidios, hechos que motivaron su inclusión en la Constitución alemana de posguerra; la primera legislación de protección de datos a nivel mundial fue aprobada en Alemania en el estado de Hesse en 1970[25], una ley sobre tratamiento de datos personales con el fin de ofrecer protección a las personas físicas ante el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del *Land* alemán, los municipios y las entidades locales rurales, así como las personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal[26]; para garantizar su cumplimiento se creaba, por la misma ley, el papel de Comisario de Protección de Datos, con independencia para el desarrollo de sus funciones. Esta ley representó el germen de la primera normativa a nivel nacional en Alemania, la Ley Federal de Protección de Datos de 1977 (*Bundesdatenschutzgesetz*), un **hito histórico**. De esta misma época es la *Data Lag* 1973/289, por la cual Suecia regulaba los bancos de datos personales relativos a personas físicas, desarrollados por medios automatizados, exigiendo la previa autorización y la asociación a una autoridad de control (la *Datainspektionen*), una especie de Ombusman referido al tratamiento de datos con responsabilidad para velar por el cumplimiento de la ley, con distintas facultades; inspectoras, normativas e incluso procesales para solicitar la aplicación judicial de sanciones. Similar a la regulación alemana, la ley sueca preveía un amplio espectro de ilícitos que podían recibir sanción penal con penas alternativas de multa y privativas de libertad.

Esta primera fase centró la protección fundamentalmente en la regulación de las bases de datos, con escasos reconocimientos de derechos a los titulares de los datos registrados. Posteriormente, en una segunda

[22] Para Craig y Ludloff (2011) apuestan así por la teoría del control de los individuos en el modelo europeo.

[23] La sección 1 del artículo 8 reconoce específicamente que *"todo el mundo tiene derecho al respecto de su vida privada y familiar, de su hogar y correspondencia"*.

[24] En España el artículo 18 de la Constitución de 1978 recogió en su apartado 1 que "*se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"; el apartado 4 también recoge 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"*.

[25] Bennet y Raab, 2006.

[26] Las leyes de protección de datos. Recuperado de http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14338%2526ISID%253D507%2526PRT%253D14331,00.html. Último acceso 2 octubre de 2016.

fase[27], a raíz de los avances tecnológicos y el desarrollo de la informática (con su mayor capacidad de almacenamiento de datos), se generan nuevas leyes que derivan su atención de las bases de datos hacia la concesión de derechos a los titulares de los datos, a saber, derecho de información, acceso, rectificación y cancelación de sus datos[28]. Y adicionalmente aparece una novedad, ofrecer garantías frente al tratamiento de los llamados datos sensibles; se trata de la *Loi n.º 78-17 du 6 janvier relative à l informatique, aux fichiers et aux libertés*, aprobada en Francia en 1978. La *Privacy Act* de EE.UU. es de 1974.

El primer instrumento internacional que regula la protección de datos personales desde una perspectiva que trasciende a cualquier legislación interna (y cuyo contenido influirá en distintas legislaciones europeas a partir de las década de 1980[29]) es el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de la Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal (ver apartado 2.2.2.). Se trata del **primer paso global para disponer de una normativa transnacional tendente a una armonización.**

A partir de entonces la UE asumió su responsabilidad en protección de datos, un camino en esta materia que condujera al correcto funcionamiento de un mercado unificado; la protección de datos armonizada parecía un objetivo a alcanzar para consolidar la Comunidad Económica Europea. El flujo de información y datos personales debía quedar libre de cualquier obstáculo en el contexto paneuropeo. Las normativas más restrictivas de países como Francia y Alemania, podían representar un problema para la transferencia de datos entre Estados miembros. Para levantar barreras internas en un mercado europeo unificado, la política asumida en el seno de la UE fue aprobar una norma común, y así nació 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.

Así se desarrolló una normativa adaptada a la Directiva en cada Estado miembro, en España la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD); se refiere expresamente a los datos de salud (considerándolos especialmente protegidos y limitando la posibilidad de su recopilación y cesión), aunque sin definir su concepto. Esta ley sí describe como dato personal "cualquier información concerniente a personas físicas identificadas o identificables", asumiendo de este modo que cualquier dato que haya sido disociado o anonimizado debidamente no estará sujeto a la protección de la LOPD (ver apartado 2.2.3.).

[27] Ramiro (2008) habla leyes de segunda generación recién a las elaboradas tras la aprobación del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de la Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal; estas leyes se caracterizaron por una determinación hacia la simplificación, con abandono de los mecanismos previos de control y con la búsqueda de la autorregulación, de un equilibrio entre la protección de los derechos de los individuos y el desarrollo de las nuevas tecnologías; esta fase destaca también por la inclusión de los llamados "datos sensibles", por el reconocimiento y la tutela de los derechos de los titulares de los datos, y por la incorporación en algunas Constituciones de los Estados miembros del derecho a la protección de datos personales.

[28] Silva (2003).

[29] Gregorio (2004).

Veinte años después de la Directiva se ha hecho necesario unificar la HCE (ver apartado 2.1.4.) de los pacientes, que sea única y compartida; el éxito de la HCE depende de la identificación única de pacientes, de profesionales y centros; se necesitan profesionales (incluidos ingenieros) que conozcan la legislación sanitaria y la de protección de datos. El marco legal asegura a los pacientes que sus datos van a ser tratados con confidencialidad, y debe validar los actos de profesionales sanitarios e instituciones que desarrollan programas de salud electrónica. Independientemente de la política de acceso aplicada por los que diseñan las HCEs, el control de acceso es gestionado por usuarios y profesionales médicos en la mayoría de los sistemas de salud, dejando patente el derecho del paciente a controlar su información.

Hay que definir una cultura común de protección de datos y mejores prácticas; utilizar estándares que garanticen la seguridad y confidencialidad de la información; Sánchez-Menaremos, et al. (2014). El potencial de la HCE es inmenso si se piensa en términos de una eficiente gestión del conocimiento: el análisis de la información de pacientes, generada por los profesionales durante el proceso asistencial en un centro médico; **sin una política de protección de datos armonizada parece que la HCE unificada no será posible.**

Capítulo 1. Objetivos y metodología de la investigación.

Se hace necesario definir las motivaciones para llevar a cabo este trabajo de investigación en este preciso instante, en el contexto del Big Data y el desarrollo de la protección de datos, ahora que las nuevas herramientas tecnológicas han puesto en duda la viabilidad de una efectiva protección de datos de carácter personal, en muchos ámbitos sectoriales, y muy especialmente en el de la salud. Se quiere confirmar cuál es el modelo europeo y, como ciudadano europeo, debo preguntarme si nuestro sistema regulatorio actual (el más respetuoso a escala global con los derechos del individuo) es un modelo a seguir o si por el contrario se impone un modelo más flexible, en un momento de creciente crisis de valores como la privacidad.

1.1 Introducción.

1.1.1. Entre la Utopía y la sociedad vigilada.

El escritor y abogado Tomás Moro, de cuya muerte se cumplen 500 años en el año 2035, publicó en 1516 en la ciudad de Lovaina, exiliado del Reino Unido, su novela "Utopía"; una isla en la que reinan la paz, la justicia, la igualdad. Esta novela recoge la aspiración del ser humano a vivir en un mundo mejor, más justo, donde se garantice la igualdad (Withington, 2016; Logan y Adams, 2016).

Hoy gracias a los avances de la tecnología hemos alcanzado a vivir en la sociedad de la transparencia, del infierno de lo igual, una nueva forma de llamar a la uniformidad (Han, 2013[30]); la transparencia que lleva a la exposición, a la visión total, donde no queda espacio para la opacidad. Es la sociedad expuesta donde cada individuo es su propio objeto, todo está a la vista, desnudo.

No sorprende por tanto que algunos investigadores se pregunten si tal vez nos estamos quedando sin privacidad (Ziegele y Quiring, 2011); si el mantenimiento de una esfera privada, especialmente en entornos de Internet, se ha convertido en un lujo (Papacharissi, 2010), ahora que la comunicación en las redes sociales desempeñan cada vez un papel más relevante en la vida cotidiana de las personas (Lundby, 2009), una comunicación directa, donde como defiende Vázquez Rocca (2015) estamos sometidos a una vigilancia que interviene a través de la aparente transparencia que ofrecen hoy las nuevas tecnologías. Vivimos por lo tanto en tiempos de permanente vigilancia a través de lo que algun investigador llama "ventanas hacia el alma" (Marx, 2016).

[30] Byung-Chul Han es un filósofo y ensayista de origen coreano, que estudió filosofía en la Universidad de Friburgo, y literatura alemana y teología en la Universidad de Múnich. Se doctoró por la Universidad de Friburgo en 1994 con una tesis sobre Martin Heidegger, y actualmente es profesor de filosofía y estudios culturales en la Universidad de las Artes de Berlín. Algunos de sus libros más célebres son: La Sociedad del Cansancio; La Sociedad de la Transparencia; La Agonía de Eros; En el Enjambre y Psicopolítica: Neoliberalismo y Nuevas Técnicas de Poder (Vásquez Rocca, 2015, analiza en profundidad su obra y pensamiento).

Como recuerda Greenwald (2013), ya a mediados de la década de 1970, el Congreso de los EE.UU. investigó por primera vez las actividades de vigilancia del gobierno estadounidense, aunque el mandato de la NSA no abarcaba, en aquel momento, que su aparato de vigilancia se aplicara a nivel nacional. Cuando finalizó la investigación, el senador demócrata de Idaho, Frank Church, quién presidió el comité de investigación, ya avisó de la trascendencia futura que podría alcanzar esta vigilancia: "La capacidad de la NSA en cualquier momento podría ser rechazada en el pueblo estadounidense y ningún estadounidense tendría privacidad, tal es la **capacidad de controlar todo**: conversaciones telefónicas, telegramas, no importa"[31].

Los EE.UU. difieren mucho de la UE en lo relativo a la protección de datos personales. Esta brecha se ha ampliado desde el 11 de septiembre de 2001. De acuerdo con Hatfield (2016) se puede decir que en el modelo norteamericano defiende la priorización de la seguridad sobre la privacidad o vida privada, pero también hay diferencias inherentes en la estructura básica del régimen estadounidense (sistema sectorial, efecto post-9/11, y el escepticismo de la UE); ver apartado 3.2.1.

Para mayor complejidad de los sistemas, estamos entrando, o más bien hemos penetrado ya, en la era del Big Data, donde las tecnologías de la información en manos de empresas y gobiernos permiten recoger miles de datos de carácter personal con multitud de fines, poniendo así en riesgo esos principios básicos universales de justicia e igualdad; así nos enfrentamos a denuncias como las del excontratista de la CIA, Edward Snowden (Vázques Rocca, 2015; Greenwald, MacAskill y Poitras, 2013) respecto a la intrusión de la Agencia de Seguridad Nacional de EE.UU. (NSA) en la vida cotidiana de millones de ciudadanos, incluidos los europeos, con programas de vigilancia gubernamental y monitorización de datos como el llamado *"Owning the Net"* (Gallagher y Greenwald, 2014; Greenwald, 2013). Mientras se consolida el derecho fundamental a la privacidad, crece la necesidad de garantizar en el ciberespacio tanto la seguridad nacional como los derechos individuales (Guarino, 2014). Queda patente que hoy, bien en calidad de ciudadanos, consumidores, pacientes o individuos, estamos en las manos de nuestros gobiernos y de los gigantes de Internet (Fuchs, Boersma, Albrechtslund y Sandoval, 2013). Curiosamente, ya en 1949 George Orwell publicó su novela "1984" (hoy más que nunca de actualidad), donde anticipaba un mundo sin derecho a la privacidad, donde el gobierno usa la vigilancia y la desinformación para controlar a los ciudadanos, anulando cualquier referencia al individualismo (Orwell, 1990)[32]. En su obra "Sin un lugar donde esconderse" (resulta muy descriptivo el título en sí mismo), Greenwald (2014) defiende que la historia nos enseña que la mera existencia de un sistema de vigilancia a gran escala, independientemente de cómo se

[31] El gran hermano que menciona Rincón (2013).

[32] La sociedad vigilada y observada que señala Rincón (2013).

haga uso de él, basta por sí mismo para reprimir a todos los que no piensan del mismo modo; una sociedad consciente de estar sometida a vigilada de forma permanente se torna rápidamente "dócil y timorata".

Conviene señalar aquí que curiosamente la obra de George Orwell nace después de la II Guerra Mundial, cuando surge el denominado **"Club de los cinco ojos"**[33], precisamente a partir una estrecha relación en materia de espionaje entre EE.UU. y Reino Unido (durante la propia guerra), cuando el británico Bletchley Park trabaja para descifrar los códigos de alemanes y japoneses; a partir de aquí surgió la alianza UKUSA (antes denominada BRUSA), para compartir información de inteligencia; en secreto durante varias décadas, este acuerdo entre servicios de inteligencia occidentales se hizo público recién en 2010. Con la Guerra Fría habían surgido el Cuartel General de Comunicaciones del Gobierno Británico[34] y la NSA; se trató de una cooperación muy estrecha, que años más tarde se abrió a otros tres países anglosajones, Australia, Canadá y Nueva Zelanda, conformando el "Club de los cinco ojos".

Así todo, hoy en día podemos decir que poco sorprende la vigilancia permanente (con obtención de una cantidad ingente de datos con fines diversos), que también se desarrolla a través de lo que se podría llamar **chivatos tecnológicos**, al adquirir los ciudadanos libremente ordenadores, teléfonos móviles, tabletas, abonos de transporte, tarjetas bancarias inteligentes, tarjetas comerciales de fidelidad, localizadores GPS, etcétera (Ramonet, 2016).

A raíz del 11S y del caso Snowden, las revelaciones sobre vigilancia masiva y acceso a datos y actividades de gobiernos y particulares, se gesta el nacimiento de alguna teoría que revela los cambios fundamentales a los que estamos asistiendo actualmente; el continuo avance de la tecnología, acompañado de la creciente relevancia de la seguridad internacional; así la protección de datos está cristalizando, según algún investigador, como una norma de **derecho internacional consuetudinario** (Zalnieriute, 2015).

Cicuéndez (2015) habla muy acertadamente, aunque en otro contexto, de derechos irrenunciables e inalienables por su carácter esencial y existencial, tal vez hoy más que nunca, pues si atendemos a Han (2014) y a su "dataísmo", el Big Data nos acerca a patrones de comportamiento colectivos (de los que individualmente seguramente no somos conscientes) donde la psicopolítica digital puede tener la capacidad de adueñarse del comportamiento de las masas de tal forma que escapa a la conciencia. En este sistema, defiende Han, el individuo está sometido pero no es consciente de dicho sometimiento, el psicopoder logra que el individuo se crea libre, pero en realidad es ese sistema el que está explotando sus libertades. Para él "la psicopolítica se sirve del Big Data el cual, como un Big Brother digital, se apodera de los datos que los

[33] BBC. Escándalo de Espionaje: qué es el club de los cinco ojos. Recuperado de: http://www.bbc.com/mundo/noticias/2013/10/131030_internacional_estados_unidos_espionaje_reino_unido_club_cinco_ojos_az. Último acceso 3 enero 2017.

[34] GCHQ son sus siglas en inglés.

individuos le entregan de forma efusiva y voluntaria. Esta herramienta permite hacer pronósticos sobre el comportamiento de las personas y condicionarlas a un nivel prerreflexivo. La expresión libre y la hipercomunicación que se difunden por la red se convierten en control y vigilancia totales, conduciendo a una auténtica crisis de la libertad". Se trata del panóptico digital del que habla Vázquez Rocca (2015) en referencia a la visión común que comparte con Han, una **vigilancia que interviene a través de la transparencia a la que se nos expone en las redes sociales**. Ver el apartado 2.4.2. que aborda el proyecto PRISM de la NSA donde intervienen todos los grandes proveedores de Internet en la actualidad.

1.1.2. El individuo y el control de los datos.

El individuo ha tomado un protagonismo muy destacable en la era del Big Data, de tal forma que la revista TIME hizo la elección de "*You*" (tú/usted) como protagonista de su portada en 2006[35], reconociendo así a los millones de personas que como usuarios, de forma anónima muchas veces, utilizan Internet de manera usual (sea vía blogs, YouTube, MySpace, Facebook, Wikipedia, etcétera) y contribuyen a generar contenido. Pocos años después, en 2010, la misma revista eligió a Mark Zuckerberg como persona del año. Y al "*Protester*" (manifestante) en 2011. Todo un dato indicativo de cómo han evolucionado no sólo los tiempos y la tecnología, sino los continentes y las ideas. La tradición que comenzó la revista Time en el año 1927 con Charles Lindbergh como "hombre del año", continúa hoy, aunque se transformó en 1999 cuando paso a llamarse "persona del año"; se trata de un número especial (anual) de la revista de noticias estadounidense que destaca la vida y obra de un personaje (hombre o mujer, pareja o grupo, idea o lugar o máquina que mayor influencia hayan tenido en el ejercicio en cuestión, sea para bien o para mal de la humanidad).

Charlos Lindbergh fue el primer piloto que cruzó el océano Atlántico **uniendo dos continentes, América y Europa** -con un vuelo en solitario sin escalas-. Hoy, casi 100 años después nos hemos encontrado en la portada dedicada al año 2016 con Donald Trump como protagonista, un personaje que encarna numerosos temores sobre el futuro de las libertades y derechos individuales, reconocidos por la misma revista hace sólo unos años. Pero más aún, estos acontecimientos podrían acrecentar la brecha existente entre Europa y los EE.UU. en materias relativas a la privacidad y la protección de datos (que por otro lado abren una interesante línea de investigación futura sin lugar a dudas).

Precisamente estas materias están más de actualidad que nunca, en la era digital, donde importantes protagonistas (las grandes multinacionales de Internet), que juegan un papel importante en el respeto de los

[35] Magazine, T. (2006).

derechos individuales, proceden de los EE.UU[36]. Ya en 1982 TIME eligió al ordenador personal como "máquina del año" (frente al tradicional título de "hombre del año"), algo que nos anunciaba el inicio de la revolución del Big Data. En 1980 Bill Gates[37] ya soñaba con una meta: "una computadora en cada escritorio y en cada hogar"; en la década de los años 80 del siglo pasado se realizó un avance real por parte de compañías como Microsoft, pero también IBM, Amstrad, y Apple, por ejemplo, que se hicieron cargo de la fabricación y la programación. Así los ordenadores fueron teniendo sentido, con tamaños más pequeños y con precios más asequibles.

En este sentido la revista TIME fue pionera en su momento, pues cuando concedió el título de su portada a la frase *"the computer moves in"* (llega el ordenador personal) los usos eran todavía muy limitados tanto funcionalmente como geográficamente, y sólo tímidamente comenzó a sustituir a las máquinas de escribir. Desde la perspectiva actual, la predicción de Bill Gates parece un eufemismo y no demasiado ambicioso, pues la evolución ha sido tan veloz que transcurrió poco tiempo antes de que se hiciera realidad.

Por otro lado, en 2014 TIME seleccionó a los combatientes del Ébola como persona del año; en 1996 el hombre del año fue el Dr. David Ho, investigador del SIDA. Si ponemos estos hechos en contexto (TIME hace referencia al siglo XIV como la época de la peste bubónica, al siglo XVI que trajo la viruela al nuevo mundo, y a la gripe que se agravó a principios del siglo XX)[38]; la idea de que un virus o una bacteria pueden cambiar el mundo (y que los hombres y mujeres que luchan contra ellos también pueden) es hoy tan cierta como entonces. La misma editora de TIME, Nancy Gibbs, señaló en 2014 que el brote de Ébola de ese año había posicionado nuevos héroes en primera fila, a la vez que planteaba la pregunta de cómo el mundo puede convertir sus sacrificios personales en nuevas formas de combatir el virus, responder a las epidemias y atender a quienes más lo necesitan. Hoy el SIDA y el Ébola lideran los rankings de las enfermedades más aterradoras del mundo, pero el SIDA, que suponía una sentencia de muerte entonces, ha reducido enormemente su impacto. A pesar de ello, 20 años después de que el Dr. David Ho protagonizara la portada, todavía no existe una vacuna contra el SIDA, sin embargo el progreso ha sido sustancial gracias a los investigadores del SIDA, para lo que ha sido necesario recurrir a la investigación con datos de carácter personal de pacientes, sin los cuáles hubiera sido imposible avanzar hacia una vacuna, cada día más próxima.

El carácter emergente de la preocupación a nivel de salud pública (Pérez-Molina, Álvarez-Martínez y Molina, 2016; Suárez Conejero, 2013; Medina-Mora, Real, Villatoro y Natera, 2013) bien sea referido a

[36] Así, Microsoft (como otras compañías que operan en Internet) ha sido acusada de monopolio, como recoge Moreno (2016) y Apple ha sido investigada por la Secretaría de Comercio de EE.UU. (Reuters. U.S. FTC asking Apple about health data protection. Recuperado de http://www.reuters.com/article/us-apple-ftc-exclusive-idUSKCN0IX2I520141113. Último acceso 10 de diciembre de 2016).

[37] Moreno (2016) recuerda que Bill Gates fundó Microsoft Corporation tan sólo en 1975 con su socio Paul Allen, y fue en Albuquerque en Nuevo Méjico, para trasladarse luego a Redmond, en el estado de Washington, en 1978 (donde su objetivo se hizo realidad).

[38] Person of the Year. Recuperado de http://time.com/3627996/david-ho-person-of-the-year/. Último acceso 13 de diciembre de 2016.

materias (tan dispares) como la drogadicción, el estado de los refugiados o cualquier otra circunstancia que acompañe al individuo, unido a la trascendencia de esta peligrosa evolución, deben hacernos reflexionar muy seriamente. Según Castells (2001) son los propios usuarios los que modifican constantemente la tecnología y las aplicaciones de Internet. ¿Pero hemos perdido los individuos el control sobre nuestros datos de carácter personal (Ramonet, 2016)? ¿está en riesgo la libertad individual en beneficio de grandes compañías y poderosos gobiernos con ilimitados recursos (Beck, 2013)? ¿cómo afectará esta revolución de datos al sector de la salud en los próximos años (Dyke, Dove y Knoppers (2016)? ¿la alianza de aseguradoras con gigantes de Internet o incluso con administraciones públicas (en casos como las llamadas *"smart cities"*) nos hará perder derechos (Edwards, 2016)? Parece que la amenaza es real.

He querido planterame si como ciudadanos y pacientes mantenemos algún control sobre nuestros datos de carácter personal más sensibles o se puede decir que prácticamente todas las compañías recolectan tantos datos de carácter personal como sea posible, aprovechando la ignorancia del consumidor y la propia inercia (Arnold, Hillebrand y Waldburger, 2015). Desde un punto de vista humanista, y con mucho acierto a mi parecer, Vásquez Rocca (2015) investiga en detalle la obra del filósofo Byun-Chul Han acerca de la sociedad de la transparencia y las nuevas técnicas de poder, para explicar la evolución "de lo viral-inmunológico a lo neuronal-estresante" en relación con el individuo como sujeto de rendimiento: "el hombre contemporáneo se ha convertido en una fábrica de sí, hiperactiva, hiperneurótica, que agota cada día su propio ser diluyéndolo en un afán competitivo"; la sociedad de la transparencia lleva hoy a la información absoluta, y permite (si cabe) pocas lagunas de información o de visión, mientras acelera el flujo de datos empíricos. El mundo parece más que nunca un gran mercado donde se exponen, venden y consumen todos tipo de datos que pertenecen a nuestra más íntima integridad como ser humano.

La situación que se está produciendo actualmente es similar a la que se vivió en el siglo XV a raíz del descubrimiento de la imprenta por Gutenberg; la imprenta liberó el conocimiento del control de las élites, hoy las nuevas tecnologías están llamadas a democratizar la medicina (Topol, 2015), de forma que los pacientes tengan un mayor control sobre sus datos frente a un **régimen médico paternalista donde *"the doctor knows best".*** La comunicación hoy es directa, sin intermediarios (como recuerdan Vázques Rocca y Han) pero con tensiones entre lo público y lo privado.

Como ciudadanos europeos debemos preguntarnos si nuestra regulación actual en Europa, la más respetuosa con los derechos del individuo, es un modelo a seguir o si por el contrario se impone un modelo más flexible. Hay muchos elementos que han intervenido en la evolución de *eHealth* creando campos de estudio que se podrían calificar de independientes como mHealth (Sunyaev, Dehling, Taylor y Mandl, 2014; Fiordelli, Diviani y Schultz, 2013;), gracias al desarrollo de las TIC (tecnologías de la información y de comunicación) en los últimos años. Las TIC han supuesto la mayor revolución hasta la fecha, han

representado una transformación profunda de la sociedad (Martínez, 2014; Carneiro, Toscano y Díaz, 2009); para algunos autores se trata de la "Revolución de las TIC" (Villanueva, 2011), y más concretamente de la etapa del simio informatizado (Aguilera, 2001). Las TIC están cambiando prácticamente todos los aspectos de la vida (Machado, 2000), por ello estamos ante algo más grande que una revolución: ante una nueva etapa de la humanidad, más importante aún que la revolución industrial o la aparición de la imprenta.

El tradicional paradigma paternalista de la medicina, desde los hipocráticos hasta hace pocas décadas, ha evolucionado claramente hacia un modelo autonomista, donde tomar decisiones que afectan a la vida y a la salud, ya no dependen del profesional médico de forma prácticamente exclusiva, sino que las decisiones son compartidas entre distintos actores: equipo profesional de salud y médico, paciente y posiblemente con toda seguridad personas allegadas, importantes para el paciente. Se trata de una proceso donde todas las personas que intervienen y que no son médicos pueden aportar y aportan *"de facto"* su visión, principios, creencias, sentimientos, valores y preferencias; conviene atender en este punto a los principios, reglas y conceptos bioéticos que a juicio de Manzini (2015) están implicados y enmarcan en forma apropiada este tipo de decisiones relativas a la vida y a la salud. En cuanto a los fundamentos bioéticos, estos juegan un papel importante en el tratamiento del estado de salud; algo vinculado a las metas de la medicina, el sujeto en medicina y la llamada toma de decisiones compartida hoy en día. Pues todo tiene un único fin: "**preservar y restituir la integridad personal, dañada por la enfermedad"**; las situaciones del final de la vida plantean conflictos entre sacralidad y calidad de vida y el principio de proporcionalidad. Subyacen pues otros índices de resultados de la acción asistencial como por ejemplo los de riesgo/beneficio, coste/beneficio, y el concepto de posible inutilidad (futilidad) terapéutica.

Bollier y Firestone (2010) en su informe para el Aspen Institute en Washinton D.C. (EE.UU.) "*The promise and peril of big data*" hablan de *Health 2.0* como **movimiento colaborativo** en materia de salud; creen que las páginas web enfocadas al paciente representan una fuerza creciente.

1.1.3. Las redes sociales: el nuevo ágora.

Se abren nuevas vías de comunicación y de intercambio de información, Internet y las redes sociales operan como un **nuevo ágora pública de comunicación** (Area-Moreira y Ribeiro-Pessoa, 2012): muchos usuarios denominan la web 2.0 como una red social puesto que nos permite estar en contacto permanente con otros usuarios y de esta manera facilita la construcción de comunidades o grupos de comunicación horizontal (Flores, 2009; Haro, 2010). Conviene aquí recordar que el ágora griega (como centro de comercio, cultura y vida social) tuvo su equivalente romano en el foro, pero éste tenía un carácter "más solemne y menos democrático" (Hauser, 1969). En el ágora la democracia residía en la participación activa

de los ciudadanos (Damiris y Wild, 1997); Internet ofrece un gran potencial para acceder a la información y para la comunicación directa, de aquí deriva la aparición del término **Salud 2.0** que permite la información directa al paciente, y que abarca la necesidad de integrar la seguridad de los contenidos de salud con las oportunidades para interactuar que ofrece la web 2.0 (Barrionuevo y Basagoiti, 2009). Para ello habrá que superar todavía numerosas barreras pues hoy todavía no todos los ciudadanos tienen acceso o acceso en libertad a dicho ágora (debido a factores como la fractura digital, la monitorización, el bloqueo digital, etcétera).

Por otro lado conviene aquí insistir en la necesidad de considerar el derecho a la protección de datos como pilar fundamental del sistema democrático (Mañas, 2009), al tratarse de un derecho que es la base fundamental para el desarrollo efectivo de otros muchos derechos hoy día plenamente aceptados en cualquier sociedad democrática, tales como la no discriminación, la libertad de residencia y circulación, la igualdad, el derecho al trabajo, etcétera, en general está intrínsecamente relacionado con el respeto a la propia dignidad humana. La Directiva 95/46/CE de protección de datos tiene que ser interpretada por tanto a la luz de los derechos fundamentales, parte de los principios generales del Derecho comunitario. Mañas reivindica el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) "al tiempo que enuncia, en su apartado 1, el principio de no injerencia de la autoridad pública en el ejercicio del Derecho a la vida privada, admite, en su apartado 2, que una injerencia de este tipo es posible en tanto en cuanto esté 'prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás'" (apartado 71).

Conviene analizar así la jurisprudencia europea, casos que Mañas (2009) toma como referencia para analizar la relación entre la protección de datos y el acceso a la información en el derecho comunitario: la sentencia del Tribunal de Justicia de 20 de mayo de 2003, el caso Rundfunk; la sentencia Rundfunk señala que en el tratamiento de datos de carácter personal son de aplicación los **principios relativos a la calidad de los datos** recogidos en el artículo 6 de la Directiva 95/46/CE, así como los principios relativos a la legitimación del tratamiento de datos incluidos en su artículo 7; los principios de finalidad y proporcionalidad son dignos de mención, y el hecho de que según este artículo 7, letras c) y e), "el tratamiento de datos personales es lícito, respectivamente si, 'es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento', o si 'es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento [...] a quien se comuniquen los datos'" (apartados 65 y 66 de la sentencia).

Las redes sociales juegan un papel importante en materias específicas de salud, así Low-Beer y Stoneburner (2004) investigan la comunicación del SIDA como enfermedad a través de las redes sociales como catalizador de los cambios de conducta en Uganda. Los investigadores concluyen que la comunicación en las redes sociales es fundamental para prevenir enfermedades, como el SIDA, donde la comunicación vertical debe basarse en la prevención en el entorno local y la comunicación horizontal en la influencia de la conducta (Moreno Reyes, 2015). En general la comunicación debe ejercer diversas acciones puntuales y debe movilizar; Castells (2012) analiza los elementos de convergencia de los diferentes movimientos sociales (a través de las redes en Internet) y su capacidad transformadora y generadora de cambio. Coincido con Castells en que a través de las redes interactivas de comunicación es como los individuos se conectan fácilmente entre sí, y esta herramienta les permite compartir...Internet se así convierte en un soporte material, que permite no sólo organizarse, sino deliberar y coordinar acciones, y por supuesto decidir. Este planteamiento que Castells aplica a los **movimientos sociales en la era de Internet**, referido especialmente a la primavera árabe, resulta muy útil para el contenido de esta investigación, pues es perfectamente trasladable a la salud, en países desarrollados (por ejemplo de Europa) o en otros en desarrollo como sería el caso de Latinoamérica. Es más, las redes sociales *online* permiten una comunicación y acceso a la información de forma instantánea, algo que de otra manera quedaría relegado en el tiempo (por ejemplo, la visita a la consulta de un médico, a la oficina de farmacia, o el resultado de un análisis de sangre); la red social permite acceder en segundos a síntomas de una enfermedad o a curas recomendadas, pero también a posible medicación idónea o recomendada, terapias alternativas, etcétera. Castells habla de un **círculo virtuoso entre las nuevas tecnologías y la autonomía**, entendiendo que es por medio de la conexión en la red cómo los individuos ingenian su autonomía con personas de similares ideas a través de las redes que eligen; se trata de una idea de la autonomía relacionada para él con autocomunicación de masas (referido a redes horizontales en las que se intercambian mensajes de muchos para muchos, con el protagonismo de ideas como la cooperación y la instantaneidad. Sin entrar a abordar los riesgos que puede entrañar para la salud que la comunicación no esté asesorada por profesionales sanitarios, detecto en este círculo vicioso cómo circulan datos de salud que escapan fácilmente a nuestro control. Castells (2014) aborda la continua transformación de la tecnología de la comunicación en la era digital y cree que pone al alcance todos los aspectos de la vida; pero más allá y recuerda como en los últimos 40 años, con la explosión de Internet y las comunicaciones inalámbricas, la comunicación en la sociedad se ha ido desplazando desde la comunicación de masas a la **autocomunicación de masas;** esto para Castells implica cambiar el esquema tradicional de comunicación social (donde un único mensaje es enviado de una persona a muchas, con muy poca interactividad) por otro mucho más dinámico, un sistema fundamentado en mensajes de muchos a muchos (se puede considerar multimodal), donde los emisores son receptores y viceversa.

Con todo ello, estamos asistiendo hoy en la sociedad a una comunicación cada día menos de arriba y en cambio más bien de abajo hacia arriba (Mylona, 2008; Gibson y Rommele, 2008; Gibson, Ward y Lusoli,

2002), en distintos ámbitos, pues son los propios individuos quienes comparten ideas y proponen soluciones a través de las redes sociales. El poder de distribuir y comentar los mensajes de salud podría pasar aún con más frecuencia de unos cuantos expertos a los individuos o receptores del mensaje. Por lo tanto, la comunicación en *eHealth* podría desarrollarse de forma más interactiva, donde el receptor está cada vez más en la posición de determinar y alterar -al compartir, comentar y aprobar- en qué forma los mensajes relativos a la salud podrían llegar a otros destinatarios; así podría cambiar de forma definitiva lo que se ha llamado un proceso descendente (*"top-down")* en la comunicación de la salud, hacia un **enfoque "horizontal"** en esencia, como defiende Friedrich (2014).

Algo que viene a suceder en paralelo al crecimiento, especialmente en *eHealth*, del concepto emergente conocido como M2M *("machine to machine")*[39], cuya madurez llegará con el desarrollo de **plataformas horizontales**, de acuerdo con la definición que hacen de él Boswarthick, Elloumi y Hersent (2012). El ETSI es el *European Telecommunications Standards Institute* (Instituto Europeo de Normalización de las Telecomunicaciones)[40], organism que juega un papel de liderazgo en el desarrollo de tecnologías de comunicación móvil, pues produce normas aplicables a nivel mundial para las tecnologías de la información y las comunicaciones (TIC), incluidas las tecnologías fijas, móviles, de radio, convergentes, de radiodifusión e Internet (sus normas facilitan el desarrollo de tecnologías como estándares para GSM, DECT, tarjetas inteligentes y la firma electrónica, y están reconocidas oficialmente por la Unión Europea como Organización Europea de Normalización). Sus miembros incluyen las compañías líderes a nivel mundial y organizaciones innovadoras en I + D; el ETSI ha regulado el M2M, en la figura 1.0. se pueden ver campos donde ya se aplica el M2M, como el de la salud (vigilancia de los signos vitales, apoyo a ancianos o minusválidos, acceso a la red de telemedicina, y diagnóstico remoto), además del sector de la seguridad, del seguimiento y rastreo, de pagos, mantenimiento / control remoto, medición, y dispositivos de consumo.

[39] Pérez-Cebollada, Martínez-Ruiz & Bernal-Agustín (2014).

[40] ETSI. Recuperado de http://www.etsi.org/about. Último acceso el 17 de diciembre de 2016.

Figura 1.0.
Ejemplos de aplicaciones M2M

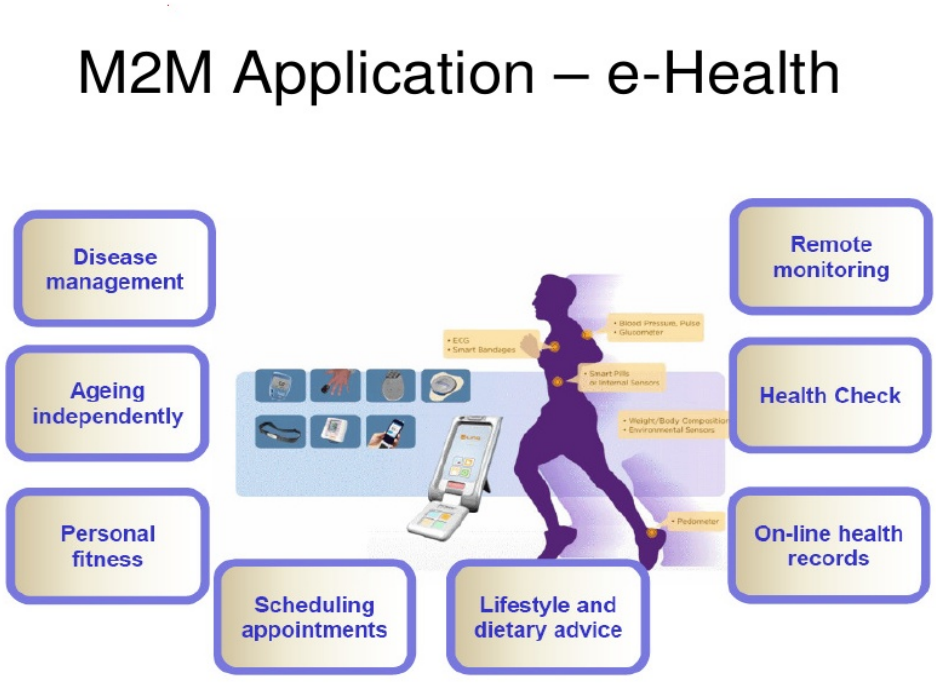
Service Area	MTC applications
Security	Surveillance systems Backup for landline Control of physical access (e.g. to buildings) Car/driver security
Tracking & Tracing	Fleet Management Order Management Pay as you drive Asset Tracking Navigation Traffic information Road tolling Road traffic optimisation/steering
Payment	Point of sales Vending machines Gaming machines
Health	Monitoring vital signs Supporting the aged or handicapped Web Access Telemedicine points Remote diagnostics
Remote Maintenance/Control	Sensors Lighting Pumps Valves Elevator control Vending machine control Vehicle diagnostics
Metering	Power Gas Water Heating Grid control Industrial metering
Consumer Devices	Digital photo frame Digital camera eBook

Fuente: datos de ETSI, *European Telecommunications Standards Institute*

En la figura 1.1. se puede apreciar la aplicación M2M a ámbitos como *eHealth*, que incluye gestión de enfermedades, estilos de vida, datos de salud *online, etcétera*. Las comunicaciones de máquina a máquina (M2M), también llamadas comunicaciones de tipo de máquina (MTC), son un elemento clave en futuras redes de datos de paquetes móviles celulares. Los esfuerzos iniciales de 3GPP (*Third Generation Partnership Project* o Proyecto de Asociación de Tercera Generación) se han enfocado en la capacidad de diferenciar dispositivos MTC, permitiendo a los operadores manipular selectivamente dispositivos MTC en situaciones de congestión o sobrecarga; 3GPP ha añadido especificaciones adicionales para integrar las

comunicaciones M2M en la red general. La industria analítica de MTC crecerá con fuerza en los próximos años; incluyendo la segmentación de los ingresos para los cinco componentes que, en conjunto, permiten el uso de analíticas en los servicios M2M: integración de datos, almacenamiento de datos, análisis básicos, presentación de datos y servicios profesionales asociados. Por lo tanto, **MTC tiene una estrecha relación con el desarrollo del Big Data**, donde cada uno contribuye al crecimiento proyectado del otro[41].

Figura 1.1.
Aplicación M2M en *eHealth*



Fuente: ETSI (European Telecommunications Standards Institute)

Es vital para una correcta armonización de dispositivos y sistemas el trabajo de los organismos de normalización[42], que pueden ser bien internacionales, regionales o nacionales; Yue, Ali, Zhang y Pradhan (2016) no incluyen en su clasificación ningún organismo nacional de normalización, con buen criterio, pues los estándares producidos por los organismos de normalización nacionales tienen intrínsecamente un campo de aplicación limitado, a diferencia de las normas internacionales y de la UE. Se trata por lo tanto de poner

[41] 3GPP. Retirado de http://www.3gpp.org/about-3gpp. Último acceso el 17 de diciembre de 2016.

[42] A principios del siglo XX da comienzo la actividad de normalización al crearse en Inglaterra el Comité de Normalización Mecánica, que dio paso al British Standards Institution (BIS) en 1918, a la vez que en EE.UU se funda el American National Standards Institute (ANSI), en Alemania el Deuteches Normenausschuss (DIN) y en Francia el AFNOR. Es España se crea IRANOR en 1946, como institución dedicada a la normalización, organismo perteneciente el Consejo Español de Investigaciones Científicas (CSIC) hasta que en 1984 pasa a formar parte del Ministerio de Industria y Energía, integrándose en la Dirección General de Innovación Industrial y Tecnología. Debido al intercambio de bienes y servicios durante la II Guerra Mundial se evidencia la utilidad de la actividad de normalización, que pasa a ser considerada como una herramienta eficaz para un desarrollo más competitivo del sistema industrial (Kress, 1986).

en valor la capacidad de las normas de la UE, entre las que destacan las producidas por el Instituto Europeo de Normalización de Telecomunicaciones, que como he indicado viene elaborando una importante cantidad de normas en relación con las TIC.

En cuanto al uso de las redes sociales y su aplicación a Internet no queda hoy espacio para la duda respecto a su influencia en muchos ámbitos de la vida y al valor de los datos que circulan en las redes; Benevenuto, Rodrigues, Cha y Almeida (2009) confirman el poder de la utilización de los datos, al analizar el seguimiento de clics para identificar patrones de comportamiento en redes sociales de Internet como Orkut, MySpace, Hi5 y LinkedIn. Read, Shah, Lupita y Woolcott (2012) analizan los datos de conducta de los *millennials* en las redes sociales. Goyal, Bonchi y Lakshmanan (2010) no sólo se centran en constatar que existe una verdadera influencia en una red social de Internet, sino que muestran cómo existen además posibilidades reales de realizar predicciones basándose en datos de la red. La alimentación también forma parte importante de la calidad de vida y la salud; Kwok y Yu (2013) investigan cómo es la comunicación de un restaurante con sus clientes mediante el uso de las redes sociales en Internet, para concluir que la actualización de la información y los mensajes visuales son lo que más influyen e incitan al consumidor.

Smith y Kristakis (2008) investigaron las redes sociales en el entorno de la salud para concluir que su información de salud está interconectada del mismo modo que los individuos lo están a través de las redes; estos autores confirman que la existencia de redes sociales significa que la salud de las personas es interdependiente, y que la salud y el cuidado de la salud pueden ir más allá del control del individuo, de forma que recomiendan prestar atención, tanto a pacientes, como a médicos, legisladores e investigadores. Kamal, Fels, Blackstock y Ho (2013) abordan las redes sociales de Internet desde la perspectiva de la salud en torno a conceptos como "*appeal"* (atracción), "*belonging"* (pertenencia) y "*committment"* (compromiso), para concluir que utilizando plataformas como VivoSpace se puede ofrecer una metodología que motive al usuario para lograr un cambio positivo en la conducta de salud.

Chou, Hunt, Beckjord, Moser y Hesse (2009) entienden que el crecimiento reciente de los medios sociales no está uniformemente distribuido entre grupos de edad, y en consecuencia creen que los programas de comunicación sobre salud que utilizan como herramienta las redes sociales en Internet, deben tener en cuenta en primer lugar la edad de la población objetiva para contribuir a garantizar que los mensajes lleguen a la audiencia deseada; si bien entre las personas con acceso a Internet existen a veces disparidades raciales o étnicas en la población objetiva, relacionadas con el estado de salud en el acceso a Internet, estos factores no afectan el uso de los medios sociales.

Hawn (2009) analiza la atención primaria a partir de un programa llamado 'Hola Salud' en Brooklyn, ciudad de Nueva York, como emblema de la medicina moderna y ejemplo de hacia donde camina

el futuro de la salud. El programa basa su gestión en las redes sociales en Internet como herramienta de comunicación efectiva y económica, utilizados por médicos y dando apoyo a pacientes con los que interactúan, a través de blogs, plataformas de mensajería instantánea, chats y vídeos, y redes sociales. McNab (2009) entra en el fondo del asunto y estudia qué ofrecen las redes sociales a ciudadanos y personal sanitario, para concluir que redes sociales como Twitter pueden no traer salud a todos, pero ciertamente pueden ayudar a aportar información precisa sobre la salud a un número muy elevado de personas, como nunca antes, pues al fin y al cabo un mensaje de emergencia sobre el brote de una enfermedad, por ejemplo, puede propagarse a través de Twitter más rápido que cualquier virus de la gripe. Se trata de una herramienta más para los profesionales de la salud.

Son varias las sociedades profesionales, entre ellas el Colegio Americano de Médicos, la Asociación Médica Americana y el Consejo Médico General del Reino Unido, que han publicado una guía para los médicos sobre el uso de las redes sociales, como recogen Crotty y Mostaghimi (2014); sus recomendaciones versan sobre la identidad del médico que asiste en las redes, el comportamiento profesional y la **seguridad de la información**. Estos autores concluyen que en líneas generales los médicos deben tratar de usar las redes sociales en Internet para el tratamiento y contacto directo con el paciente, puesto que la información puede ser accesible para terceros y puede estar controlada por terceros también, es decir, la información puede no estar almacenada de forma encriptada.

1.1.4. Los nuevos modelos de negocio.

La sociedad contemporánea se caracteriza por un entorno significativamente "condicionado por el conocimiento tecno-científico, y las tecnologías de la información y el conocimiento (TIC), elementos que generan y modulan lo que ahora se ha dado en llamar sociedad(es) del conocimiento" (Pérez y Domínguez, 2016). La noción de "sociedad del conocimiento" fue utilizada por primera vez en 1969 por Peter Drucker, y veinte años después, a partir de 1990, se profundiza en el término, como nuevo modelo que nada tiene que ver con la sociedad industrial nacida al inicio del siglo XIX, y que viene acompañada de una nueva moneda de cambio en las relaciones humanas, dejando en segundo plano los productos y los servicios; se trata del conocimiento, es decir, "la información que se asimila por un individuo y que le permite tomar decisiones y actuar", como apuntan Díaz-Hernández y Álvarez-Pérez (2016), para quienes el conocimiento se encuentra más relacionado con la acción que con los datos o la propia información en sí mismos, aunque defienden que la sociedad del conocimiento no es algo que, en su opinión como profesionales de la salud, exista actualmente, sino que es más bien una etapa evolutiva, posterior a la actual era de la información, una asignatura pendiente en el sector de la salud; se trata del uso e innovaciones de las TIC, donde el incremento

en el volumen y la transferencia de información, junto a su análisis, transforma la manera en que se desarrollan muchas actividades en la sociedad moderna.

Los sistemas de salud están evolucionando y los avances de los últimos años en la TIC revelan que en el futuro uno de los campos de crecimiento más conflictivos de las TIC, en cuanto a la gestión de los datos que afectan a personas se refiere, será el sector de la salud, un entorno tradicionalmente regulado, donde intervienen ciudadanos, pacientes, profesionales sanitarios, legisladores, proveedores, etcétera; el desarrollo en el ámbito de *eHealth* está siendo tan rápido en tan pocos años (Martínez, 2014), que está afectando a las políticas de privacidad y protección de datos existentes actualmente. **Los nuevos sistemas de salud y los modelos de negocio innovadores** exigen, ante una todavía dispar regulación, un nuevo marco de conducta (Wass y Vimarlund, 2016; Van Doosselare, Herveg y Silber, 2008).

El desarrollo de la tecnología de *eHealth* debe centrarse más en el contexto concreto al que se refiere, haciendo hincapié en lo que esta tecnología puede aportar en la práctica a las necesidades de todas las partes interesadas, recuerda Van Limburg et al. (2011); la incorporación del concepto de modelos de negocio sólo puede contribuir a crear en común y a formular un conjunto de factores determinantes de éxito, que influirán en la **sostenibilidad y la eficacia de la tecnología de *eHealth***.

Por otro lado, según Villanueva (2011) los profesionales de la sanidad se enfrentan a aspectos muy controvertidos como son los referidos a la privacidad, la confidencialidad, la seguridad y la responsabilidad legal "tanto de los nuevos flujos de información médica (p. ej., historia clínica electrónica, comunicación mediante correo electrónico, etcétera) como de las nuevas maneras de prestar servicios sanitarios (telemedicina, teleasistencia, control de los pacientes a distancia mediante dispositivos en su hogar, etcétera). En este sentido, es necesario que los avances tecnológicos y las nuevas prácticas asistenciales estén en consonancia con un marco legislativo adecuado" (Lupiáñez-Villanueva, Hardey, Torrent y Ficapal, 2010; Masters, 2008). Por todo ello, la ciberseguridad debe ser tenida en cuenta a la hora de proteger la información digital en los sistemas interconectados (y en los nuevos modelos de negocio), comprendida como parte integrante de la seguridad de la información (Elmaghraby y Losavio, 2014).

Mayer y Leis (2010) formulan un concepto interesante (que cobra cada día mayor sentido) al afirmar que "la Web 3.0 dotará de una mayor **personalización de los servicios sanitarios**, la más conveniente en cada momento y para cada persona, asegurará la interoperabilidad entre diversos dispositivos y garantizará la aplicación más eficiente de las últimas tecnologías de la información disponibles".

Un estudio global de Korn Ferry publicado en Los Ángeles recientemente[43] y referido a las percepciones de consejeros delegados destaca una **sorprendente ausencia de confianza en el valor de las personas en sus organizaciones, a la vez que están poniendo un mayor énfasis en la tecnología** y los activos tangibles; se han realizado entrevistas en profundidad con 800 líderes empresariales de organizaciones globales valoradas en miles de millones, y entre las principales conclusiones destacan las siguientes:

-Un sesenta y tres por ciento dicen que en 5 años la tecnología será la mayor fuente de ventaja competitiva de la empresa.

-El sesenta y siete por ciento señala que la tecnología creará mayor valor en el futuro que las personas.

-El cuarenta y cuatro por ciento afirma que la **prevalencia de la robótica, la automatización y la inteligencia artificial** harán que las personas sean en gran medida irrelevantes en el futuro del trabajo.

Estos resultados revelan en si mismo el creciente valor de la tecnología, no sólo en el sector de la salud en sí mismo pero en el mundo de la empresa en general, donde queda patente que **la tecnología será la herramienta que marque la diferencia entre modelos de negocio**. Además los líderes que han participado en este estudio confirman que la tecnología se está convirtiendo en el eje central de sus pensamientos y decisiones, de forma que ya ocupa entre el 40% y el 60% de sus prioridades en cuanto a la política estratégica se refiere.

La aplicación de un modelo de protección de datos tendría como objetivos concretos:

- Una mejora de la competitividad (Robles, Ramírez, Rodríguez, González y Gayo, 2014; Manyika et al, 2011).

-Una disminución de los riesgos de explotación (posibles demandas de los usuarios) y una reducción de los costes económicos de explotación de los nuevos modelos de negocio de *eHealth* (incluidas las sanciones impuestas por organismos oficiales como consecuencia de la vulneración efectiva del derecho a la protección de datos); Manning (2015), Williams (2010).

[43] Korn Ferry Global Study (17 noviembre 2016).

- Una mejora de la reputación (Manning, 2015) de los nuevos modelos de negocio (redes sociales más seguras para los usuarios), una mayor credibilidad y garantía de calidad de datos que contribuyan al incremento del número de usuarios (en la cada día mayor competencia por la captación de nuevos usuarios), al ofrecer una gama segura de productos (Terstegge, 2017).

- Sostenibilidad de los nuevos modelos de negocio (Van Limburg et al., 2011); el uso de los controles de protección de la privacidad como garantía de desarrollo de un negocio.

En definitiva, se espera definir un modelo que aporte una ventaja competitiva y beneficios colaterales al poder incluirse en un código deontológico -código sectorial o tipo recogido en el artículo 32 LOPD-[44], que proporcione un marchamo que distinga el modelo de negocio como especialmente sensibilizado con el cumplimiento de la ley y la protección de los derechos individuales. Los códigos tipo se regulan en el artículo 32 de la LOPD y en el Título VII (artículos 71 a 78) del Reglamento de Medidas de Seguridad[45]. Estos códigos tratan de adecuar las obligaciones en protección de datos a las especificidades de los tratamientos realizados por aquellos que se adhieren a ellos, mediante normas concretas que permiten armonizar los tratamientos de datos efectuados por aquellos que se han adherido a los mismos, facilitar el ejercicio de los derechos de los afectados y al mismo tiempo favorecen el cumplimiento de lo dispuesto en la LOPD y su Reglamento. Los códigos tipo deben tener el carácter de **códigos deontológicos o de buena práctica profesional**, y para ser válidos de acuerdo a la ley en España deben ser depositados e inscritos en el Registro General de Protección de Datos. Aunque tienen un carácter voluntario, son vinculantes desde la adhesión a los mismos. Los códigos tipo de carácter sectorial pueden atender a todos los tratamientos realizados por el sector, o sólo a una parte, teniendo que ser formulados por organizaciones que sean

[44] El artículo 32 de la LOPD referido a los códigos tipo estipula:

"1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas".

[45] El apartado 3 del artículo 73 de Reglamento recoge:

"En particular, deberán contenerse en el código:

a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso".

representativas del mismo, cuando menos en su ámbito geográfico de aplicación. Los códigos tipo pueden ser promovidos por una empresa y este caso tendrán que referirse a todos los tratamientos que lleve a cabo[46].

Un nuevo hito en el desarrollo de la protección de datos en el sector sanitario, especialmente en España, ha sido la inscripción en el Registro General de Proteccción de Datos, el 14 de enero de 2016, del **código tipo de protección de datos para organizaciones sanitarias privadas,** que recuerda cómo el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, estipula diferentes niveles de protección en relación a las cualidades o características de los datos, y establece una jerarquía en la cual la información que se trata diariamente en un centro sanitario (datos de salud de pacientes en su mayoría) debe quedar protegida a través de medidas de seguridad de nivel alto, con las consabidas obligaciones legales de cumplimiento que de ello se derivan.

Ahora que se acaba de aprobar el Reglamento (EU) 2016/679 de protección de datos (RGPD), se abren nuevas oportunidades para el modelo europeo de protección de datos (Mañas, Caro y Gayo, 2016), con **amplias repercusiones para todas las organizaciones que manejan datos de ciudadanos europeos, más allá de la UE.**

1.2. Aportaciones e interés del trabajo de investigación.

1.2.1. Valoración de la magnitud de los avances en protección de datos.

¿Cuáles son las razones que hacen interesante y necesaria esta investigación? Se quiere contribuir a valorar la magnitud de los avances en materia de protección de datos en la UE (Boehm, 2011), en lo que se refiere a datos especialmente protegidos como los de salud (Delgado y Sánchez, 2008; Martínez, 2007) y deja a la vista cuál será la tendencia en los próximos años en el contexto del Big Data y las nuevas tecnologías (Monleón-Getino, 2015; Tascón, 2013), en vísperas de la aplicación del RGPD . La normativa de la UE está avanzando hacia el doble objetivo de una eficiente implementación de la HCE (Fernández-Alemán, Señor, Lozoya, y Toval, 2013; Coorevits et al., 2013; Iakovidis, 1998) y la efectiva protección de la privacidad de forma armonizada (Fears et al., 2014; Coorevits et al., 2013; Joas et al., 2012) donde el ciudadano, titular de los derechos fundamentales, debe ejercer el control último; por ello la concienciación ciudadana desempeña un papel central (Delgado y Saltor, 2013), tanto respecto al alcance como al ejercicio de los derechos, pues sin ella no existirá una protección real ni efectiva; los individuos no podrán ejercer sus

[46] Qué es un código tipo en protección de datos. Recuperado de http://ayudaleyproteccion datos.es/2010/09/07/que-es-un-codigo-tipo-en-proteccion-de-datos/. Último acceso 8 de diciembre de 2016.

derechos ante las autoridades competentes o incluso ante los tribunales, siendo el Estado y sus operadores los garantes de las eficacia final de la normativa.

La información que se registra actualmente en la HCE se podría ampliar, siempre que los individuos europeos perciban que su privacidad está garantizada. Hoy la vulnerabilidad reside en los jóvenes entre 15 y 24 años que hoy parecen dispuestos a renunciar a su privacidad bien a cambio de determinados servicios (Comisión Europea, Eurobarómetro especial 359, 2011); el análisis por edad y país de procedencia de los individuos contribuye a valorar la magnitud de los riesgos. Los ciudadanos españoles aparecen entre los europeos más dispuestos a facilitar su historial clínico en Internet.

1.2.2. Interés para las start-ups.

Múltiples *start-ups* (nuevos proyectos en adelante) se están poniendo en funcionamiento cada año, se trata de nuevos modelos de negocio (Faerberg, 2016; Chesbrough, 2013; Baden-Fuller y Haefliger, 2013; Onetti, Zucchella, Jones y McDougall-Covin, 2012), y es en el sector de la salud (y en el financiero tal vez también), donde pueden residir los importantes proyectos de éxito y beneficios (Effertz, 2016; Peters, Blohm y Leimeister, 2015; Kimble, 2015), por ello la política de privacidad (al tratarse de datos sensibles) tendrá que jugar una papel relevante (Manning, 2015; Tene y Polonetsky, 2012;). La seguridad jurídica representa una ventaja competitiva para que las empresas inviertan en innovación (Robles, Ramírez, Rodríguez, González y Gayo, 2014), a la vez que la competitividad fomenta el desarrollo tecnológico (Giacometti-Rojas, 2013) y la innovación (Manyika, et al., 2011). Así, logramos el doble objetivo de que proveedores y usuarios acepten y confíen en nuevos servicios en el sector de la salud, lo que puede suponer beneficios colaterales para los nuevos modelos de negocio.

Peppet (2014) previene de la era del*"Internet of Things"* y sus riesgos, en casos como la tecnología basada en sensores, cuyo uso puede suponer un alto riesgo de discriminación por razones de privacidad, en el contexto de los dispositivos de rastreo médicos y de acondicionamiento físico, que miden, registran y analizan diferentes aspectos de la vida cotidiana; como ejemplos incluye las cintas de acondicionamiento físico que rastrean los pasos que damos cada día, las calorías quemadas y los minutos de sueño, las cintas de seguimiento de la frecuencia cardíaca, la presión arterial y los niveles de glucosa, cintas de registro del rendimiento deportivo y cintas de monitoreo del estado mental.

En concreto, conviene aquí hablar del concepto de "**patentes generadoras de datos**", que son invenciones patentadas que implican tecnologías que, por diseño, generan datos valiosos por su funcionamiento o uso (Simon y Sichelman, 2017). Por ejemplo, las pruebas genéticas y los dispositivos

médicos generan datos de los pacientes. Los motores de búsqueda en Internet y las redes sociales digitales generan datos sobre los intereses de los consumidores. Cuando se patentan invenciones generadoras de datos y el titular de la patente goza de poder de mercado sobre la invención, el titular de la patente goza "de facto" de poder de mercado sobre los datos generados por la invención, incluso una vez haya vencido la patente.

El ciudadano europeo se presenta en esta investigación sensibilizado con el cumplimiento de la ley y la protección de los derechos individuales, a la vez que los europeos se presentan a favor de que la normativa y sus sanciones se hagan efectivas desde órganos de control a nivel paneuropeo, en lugar de a nivel nacional o regional. **Este marco común se convierte en un modelo con influencias** más allá de Europa, se erige como un sistema influyente (Greenleaf, 2012).

La Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, junto con la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, otorgan competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas exigen un desarrollo reglamentario con la especialidad de que ambas normas se ordenan a la tutela de los derechos de las personas físicas, pero también de las jurídicas.

1.3. Objetivos de la investigación.

-Principal:

En el entorno actual del Big Data el objetivo principal de esta investigación es constatar una tendencia liderada por los propios ciudadanos hacia la homogeneización en Europa de los parámetros a los que se debe adecuar la salud digital en relación con la protección de datos, a la vez que el marco europeo se erige como un modelo con influencia transfronteriza más allá de la UE pudiendo considerarse un modelo líder a nivel global (Craig y Ludloff, 2011; Greenleaf, 2012).

-Secundarios:

Desarrollar y promover el conocimiento sobre los parámetros de la protección de datos en el ámbito de la salud digital, de forma que se facilite la implicación del cuerpo de médicos, ingenieros, profesionales sanitarios y demás agentes implicados, al margen de los profesionales del derecho.

Identificar barreras y ventajas de la convergencia de las políticas y normativas de terceros países con el modelo de la UE en materia de protección de datos en el campo de la salud digital.

Verificar la confianza de los ciudadanos europeos en las instituciones comunitarias para liderar el proceso de convergencia, con los mismos derechos y protecciones a nivel paneuropeo.

Constatar las razones que fundamentan la necesidad de eliminar las actuales divergencias entre Estados miembros y los costes asociados para las empresas, derivados de la transposición de la Directiva 95/46/CE, en vísperas de la aplicación efectiva del RGPD.

1.4. Proceso de trabajo seguido en la investigación. Metodología.

Esta investigación, que ha seguido una metodología, se ha organizado en tres fases:

1) La **primera fase**, partiendo de una amplia revisión bibliográfica sobre la materia para obtener una visión completa e integral, se centra en el **marco europeo** analizando la **evolución de la protección de datos hacia su plena integración** en el seno de la UE, en el contexto de la **salud** y las **nuevas tecnologías** a través de:

   a) Las **actitudes sobre la protección de datos e identidad electrónica de los ciudadanos europeos en 27 de los Estados miembros de la UE.**

   b) Comparando la cultura sobre datos de carácter personal en esos 27 países hacia la **adaptación a un marco legal armonizado.**

2) En la **segunda fase** se analizan las seis principales economías de la UE, y se **comparan las seis mayores economías de Latinoamérica**, para atender a las ventajas de la convergencia de terceros países con la política europea, y concluir con la **influencia de la regulación de la UE**.

3) Una vez analizada **la interrelación del marco europeo (Estados miembros de la UE) y latinoamericano** se concluyen **en una tercera fase las dificultades a las que se enfrenta la convergencia de terceros países**, desde el ejemplo latinoamericano, a la hora de desarrollar un marco jurídico armonizado.

En este proceso de trabajo se han podido identificar las dificultades a las que se enfrenta la convergencia con el modelo europeo (al margen de las propias diferencias culturales entre Estados miembros de la UE, en vísperas de la aplicación del nuevo Reglamento General de Protección de Datos), así como sus influencias fuera del territorio europeo. La **primera fase** ha permitido detectar el limitado interés que esta

materia ha despertado en la literatura científica hasta la fecha, revelando las dispares actitudes de los ciudadanos europeos hacia la protección de datos sensibles como los de salud. La comparativa de la cultura de protección de datos sensibles en Europa ha desvelado divergencias entre países del norte y oeste de la UE (que tienden a considerar la información médica como un aspecto que forma parte de la privacidad de las personas), mientras que en general los usuarios de Internet en países del sur de Europa, como España, Italia, Grecia y Portugal, junto con Bulgaria, tienden a revelar con mayor facilidad datos de carácter personal[47]. Los datos que revelan las fases de este método desarrollado permiten detectar dónde debe prestarse mayor atención para lograr una eficiente convergencia al margen del nuevo Reglamento (EU) 2016/679 de protección de datos. La integración técnica de los sistemas de salud es posible pero insuficiente en sí misma; la mayoría de los ciudadanos creen que deben comprender procesos para proteger la seguridad y la privacidad de los datos de cada individuo de forma común. Así, las políticas de protección de datos pasarán a ser parte integrante de los departamentos de gestión de riesgos de empresas.

En la **segunda fase** se han podido identificar las diferencias aún existentes entre las seis mayores economías dentro de la UE, a la vez que se pone en contexto la regulación marco europea con las seis mayores economías de Latinoamérica. Se han analizado las influencias del modelo europeo de protección de datos, y las razones para la convergencia.

Para acabar identificando en una **tercera fase** las barreras que se oponen a convergencia, y de esta manera a la influencia del modelo de la UE fuera de Europa, y especialmente en América Latina.

[47] Comisión Europea, Eurobarómetro especial 359 (2011).

Capítulo 2. Marco teórico.

Es de crucial importancia que ingenieros (y profesionales de la salud) conozcan las implicaciones para la seguridad y la privacidad en sistemas de salud en el contexto de IoT[48], hacia los que no dirigimos. Es necesario como paso previo un análisis en profundidad de los conceptos que han sido clave en el desarrollo de esta investigación, como son el Big Data, *eHealth*, protección de datos, la historia clínica electrónica. La telemedicina tiene su origen en 1950 pero su evolución ha revolucionado el sector sanitario hace pocos años gracias al más asequible acceso a las nuevas tecnologías, ello ha reportado multiples beneficios, desde la comunicación con el médico a la monitorización a distancia. La capacidad del Big Data y su potencial genera oportunidades pero también seria desconfianza respecto a la recogida y el uso de los datos personales. Desde la perspectiva de la investigación, se hace necesario entender los conceptos (en un proceso de reconocimiento y comprensión de la dinámica del tema) alrededor de los que gira el proceso de armonización de la protección de datos y de los sistemas de información de sanitaria (HIS[49]). Se busca interpretar las implicaciones de los cambios con la aplicación de las TIC, en el desarrollo del *eHealth* y así valorar las transformaciones e influencias del modelo europeo del derecho fundamental a la protección de datos personales. Esta definición de conceptos previos, ayudará a determinar el grado de profundidad de la investigación y a valorar el tratamiento de las conclusiones, para poder incorporarlas a futuras investigaciones que puedan dar lugar a un nuevo conocimiento.

2.1. Conceptos previos.

2.1.1. Big Data.

El término Big Data se ha acuñado hace solamente unos 20 años; en un artículo de 1997 redactado por científicos de la NASA se describía el problema que tenían con la visualización (referido a gráficos de ordenador) que "proporciona un reto interesante para los sistemas informáticos: los conjuntos de datos son bastante grandes sobrecargando las capacidades de memoria principal, del disco local e incluso del disco remoto. Llamamos a esto el problema del Big Data. Cuando los conjuntos de datos no encajan en la memoria principal (en lo básico), o cuando no encajan incluso en el disco local, la solución más normal es adquirir más recursos"[50]; en 2008, un número de destacados científicos informáticos estadounidenses popularizaron el término, vaticinando que la informática del Big Data transformaría las actividades de las compañías, de la investigación científica, de los médicos y las operaciones de defensa e inteligencia de los EE.UU.

[48] Hu (2016).

[49] Acrónimo del inglés *"Health Information Systems"*.

[50] Press, G. (2014).

Mayer-Schönberger y Cukier (2013) defienden que el término se acuñó en el campo de las ciencias, y más concretamente, a partir de la astronomía y la genética, desde el comienzo del siglo XXI, para referirse a los datos masivos. La idea era que el volúmen de datos había crecido tanto que los ingenieros precisaban nuevos intrumentos para su análisis.

Como señala Press (2014) una base de datos tradicional de definiciones autorizadas es el Oxford English Dictionary (OED); así es como el OED define Big Data: "datos de un tamaño muy grande, típicamente en la medida en que su manipulación y administración presentan desafíos logísticos significativos". Sin embargo, muchos medios de comunicación han adoptado una definición del Big Data que resulta prácticamente ser un sinónimo de "analítica de datos", aunque interrelacionado en algunos casos con la recolección de datos de carácter personal y su invasión de la privacidad; es decir, hay poder y potencial en los datos[51]. El concepto de Big Data también se aplica a todo tipo de información que no puede ser procesada o analizada por medio de herramientas o procesos tradicionales[52].

Mucho se ha debatido sobre si el Big Data no es otra forma de decir analítica. Aunque están relacionados en opinion de Brynjolfsson y McAfee (2012), que alegan una frase de Peter Norvig, director de investigación de Google: "No tenemos mejores algoritmos. Sólo tenemos más datos", defienden que el gran movimiento de datos, al igual que las analíticas, trata de obtener información inteligente a partir de datos, y traducirlo en ventajas para los negocios, pero destacan tres diferencias clave, a saber: volúmen, veracidad y variedad, es decir, lo que se ha pasado a denominarse las 3Vs, las mismas carácterísticas que según Zikopoulos y Eaton (2011) definen el Big Data.

Según Ohlhorst (2012) el Big Data no tiene tres sino cuatro características que lo definen, son las 4Vs, a saber: volúmen, variedad, veracidad y velocidad; por un lado estamos hablando de tamaño, de una gran cantidad de datos que las compañías recogen cada día, por otro lado el Big Data no sólo se refiere a datos estructurados, sino a todo tipo de datos desestructurados, bien sea en forma de audio, texto, vídeo, como secuencias de clics, archivos de registro, etcétera. En tercer lugar, la cantidad masiva de datos recopilados puede conducir a errores estadísticos o posibles malas interpretaciones, es decir, la pureza de la información es vital para su validez. Por último, para maximizar su valor los datos, deben circular con agilidad pero a la vez estar disponibles en fuentes de archivo. Algunos autores como Baro, Degoul, Beuscart y Chazard (2015) nos recuerdan que existen investigadores que añaden una 5ªV, la valorización (Dereli et al., 2014; Özdemir et al., 2013), tal vez el aspecto más relevante del Big Data, pues tiene un coste elevado poner desarrollar las infraestructuras informáticas necesarias para almacenar estos volúmenes de datos, y por

[51] Wilder-James (2014).

[52] Qué es Big Data. Recuperado de https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/. Último acceso 23 octubre 2016.

ello las empresas requieren un elevado *ROI* (retorno de la inversión) para que se pueda justificar el gasto (si no se logra extraer todo el valor de los datos, no tendrá sentido alguno ni su almacenamiento ni su gestión).

Han (2014) habla del concepto de "dataísmo" que cree describe la sociedad de hoy en día, especialmente debido a la actual capacidad de almacenar lo que se consideran grandes cantidades de datos; profundiza en el término para describir un "dataísmo digital" donde en su opinión los datos y los números no son narrativos, sino más bien aditivos. Para él, el Big Data nos acerca a pautas de comportamiento colectivas de las que no somos conscientes de forma individual, por lo que se puede afirmar que **el Big Data hace legibles los deseos de los que no somos conscientes.**

Profundizando algo más en el concepto, el uso del Big Data en general puede crear valor de cinco maneras diferentes (Manyika et al., 2011); primero, el Big Data hace que la información sea transparente y útil en un mayor número de casos; segundo, a medida que las organizaciones almacenan más datos en formato digital, pueden recopilar información más precisa y detallada y, por tanto tanto, mejorar el rendimiento; tercero, el Big Data permite una segmentación cada vez más ajustada de los clientes y, de esta forma, ayuda a definir productos o servicios mucho más adecuados; cuarto, una analítica de datos sofisticada puede mejorar de forma significativa la toma de decisions; por último, se puede utilizar para mejorar el desarrollo de nuevos productos y servicios.

Es cada vez más elevado el número de investigadores que defienden con sus trabajos las **ventajas de la aplicación del Big Data al ámbito de la medicina, la salud y el bienestar en general** (Austin y Kusumoto, 2016; Auffray et al., 2016; Janke, Overbeek, Kocher y Lévy, 2016; Monteith, Glenn, Geddes, Whybrow y Bauer, 2016; Park, 2016; Hoffman, 2016; Stuart y Davis, 2016; Cho, 2016; Chang y Choi, 2016; Dimitrov, 2016; Mayer-Schönberger, 2016; Linares Vallejo, 2016; Baro, Degoul, Beuscart y Chazard, 2015; Suciu, Vulpe, Craciunescu, Butca y Suciu, 2015; Ram, Zhang, Williams y Pengetnze, 2015; Wang, Kung, Ting y Byrd, 2015; Asri, Mousannif, Al Moatassime y Noel, 2015; Gill y Singh, 2015; Andreu-Perez, Poon, Merrifield, Wong y Yang, 2015; Monteith, Glenn, Geddes y Bauer, 2015; Zhang, 2014; Vithiatharan, 2014; Bernard, 2014; McGregor, 2013); así, el valor de los datos resulta cada día más valioso en el tratamiento de enfermedades como el parkinson, la demencia, el autismo, el trastorno bipolar, el asma...y en general en el entorno del *eHealth*, más ampliamente conocido como tecnología de información de salud; en este entorno, el *eHealth* –incluidos ordenadores, Internet, tecnologías móviles y sensores- tiene cierto potencial para mejorar la salud y mejorar la calidad de vida, reduciendo al mismo tiempo los costes. La tecnología *eHealth* permite la identificación inteligente de la información necesaria y la distribución de información en un formato personalizado que debe apoyar a pacientes y proveedores por igual, especialmente con las complejas cuestiones de la gestión de múltiples enfermedades crónicas (Nilsen, 2015). Como en cualquier ciencia, los datos son una prueba y fuente de conocimiento (bien utilizados, claro está),

por ello la habilidad de armonizar y analizar los datos facilita poder **compartir el conocimiento** en distintas disciplinas y obtener respuestas en el complejo campo de la salud pública, pudiendo entonces el **Big Data convertirse en la Caja de Pandora para la salud** (Vithiatharan, 2014).

El Big Data tiene muchos beneficios potenciales para la investigación trasfronteriza sobre la salud y el bienestar en general como defienden Espay et al. (2016), que creen en conjuntos de datos integrados para mejorar los modelos de enfermedades comunes con el fin de comprender mejor la progresión de las enfermedades raras. Austin y Kusumoto (2016) en su artículo *"The application of Big Data in medicine: current implications and future directions"* recuerdan que el Big Data también puede facilitar la detección de efectos en la población, tales como los efectos adversos de los fármacos o la aparición de co-morbilidad.

En el entorno del Big Data en *eHealth* existen oportunidades de interactuar con los pacientes más de cerca, como bien señalan Auffray et al. (2016), e importar datos desde las aplicaciones móviles de salud o dispositivos conectados. Esta interacción con el paciente dará lugar a la recopilación de información más detallada sobre estilo de vida, el entorno clínico, y la salud en general, como por ejemplo la frecuencia cardiaca y la temperatura corporal, el sueño y la gestión del estrés, la actividad física y los hábitos de nutrición etcétera; lo que evitará la exposición a riesgos potenciales y la aparición de enfermedades (Zheng et al., 2014).

La variedad de datos que se pueden obtener depende de los diferentes formatos de las fuentes de datos y a los tipos de datos; como recuerda Vithiatharan (2014) en su estudio *"The potentials and challenges of big data in public health"*, se agregan continuamente fuentes de datos adicionales, así un gran número de teléfonos inteligentes, por ejemplo, transmiten una gama variada de información a la infraestructura de red. Y a medida que se introducen nuevas aplicaciones, lo identifica también con la **génesis de nuevos formatos de datos** que pueden llevarnos de una u otra forma a un futuro "sin secretos". Como defiende Vithiatharan el Big Data puede contribuir a la mejora de la salud pública, el potencial reside en el análisis de datos en tiempo real y una investigación más rigurosa, pero existe una falta de normalización y clasificación del Big Data que puede conducir a que tenga una pobre utilidad, que sería aún más pobre si los individuos perciben que sus derechos sobre los datos de los que son titulares se vulneran. Otro desafío vital es la necesidad de las plataformas de analizar grandes candidades de datos que van en aumento. Por todo ello, se requiere en su opinión, que comparto, una correcta regulación, una normas éticas de comportamiento, barreras a la privacidad y algunas forma de normalización de la diversidad de fuentes productoras de datos y sus fines.

Raghupathi y Raghupathi (2014) en su obra *"Big data analytics in healthcare: promise and potential"* hacen constar que el Big Data grandes en salud se refiere a conjuntos de datos de salud electrónicos de un tamaño y complejidad que los convierte en difícilmente gestionables, o imposibles de

gestionar, por medio de un software y/o un hardware tradicionales, ni tampoco son susceptibles de ser gestionados fácilmente con métodos o herramientas de gestión de datos tradicionales o comunes. Afirman que el Big Data en el ámbito de la salud es abrumador, tanto por su volumen como por la diversidad en los tipos de datos y la rapidez con la que deben gestionarse.

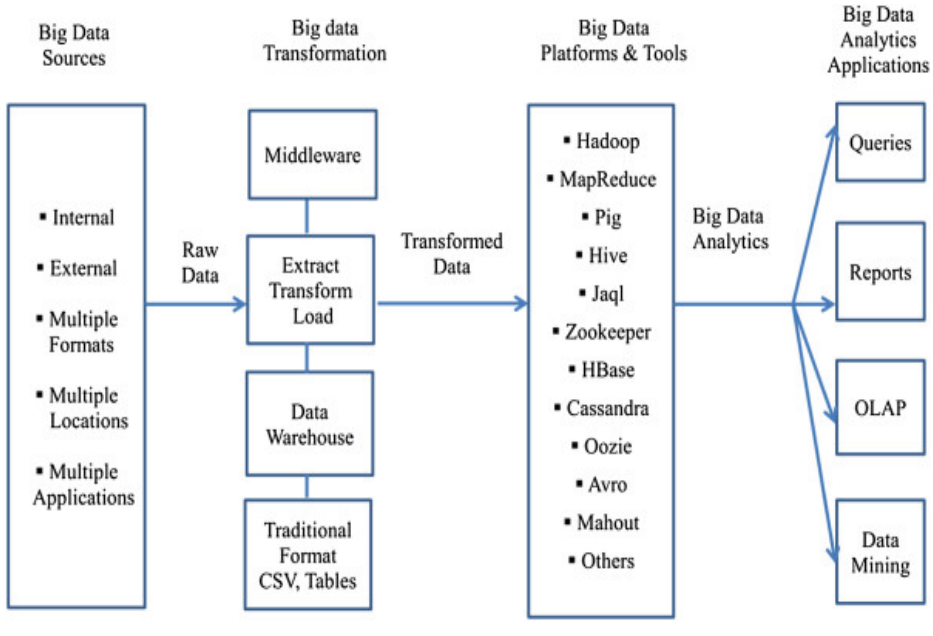
Sin embargo, Baro, Degoul, Beuscart y Chazard (2015) en su artículo "*Toward a Literature-Driven Definition of Big Data in Healthcare"* parten del entendimiento de que hasta la fecha el término Big Data no ha sido definido adecuadamente, y creen que una definición precisa, bien formada e inequívoca es un requisito necesario para una comprensión compartida del término Big Data; su trabajo trata de proporcionar una definición del Big Data en materia de salud a través de una revisión de la literatura, aunque entienden que existen errores de conceptualización cuando el Big Data se identifica con un simple conjunto de datos, o la mera reutilización de los datos; defienden que el término se usa cada vez con mayor frecuencia para referirse a conjuntos de datos, y que esos conjuntos de datos serán cada vez mayores para que se identifiquen como Big Data, debido a la misma esencia del Big Data, y este será su mayor desafío, lograr que las infraestructuras informáticas para procesarlos progresen de forma adecuada.

Auffray et al. (2016) se plantean qué es lo que se entiende hoy por Big Data, si representa sólo grandes datos o volúmenes de datos, y concluyen que existe una amplia gama de definiciones en la investigación de la salud, de forma que hablar de una definición única para todos los usos ("*one size fits all*") puede resultar demasiado ambigüo, pero sin embargo concluyen que existe una definición operativa de lo que significa Big Data en este ámbito de la investigación, o al menos un consenso de lo que significa este término (Big Data en materia de salud): aquello que abarca una información de alto volúmen, y de alta diversidad biológica, clínica, medioambiental y de estilo de vida obtenida desde un solo individuo a grandes grupos, en relación con su estado de salud y bienestar, en uno o varios momentos en el el tiempo. El Big Data al qie se refieren Auffray et al. (2016) sólo puede ser tratados mediante la adopción de un sólido modelo de gobierno y buenas prácticas de nuevas tecnologías, es decir, compatible con los estándares de calidad aceptados de forma genérica junto con el almacenamiento de datos interoperables, la integración de los datos y con soluciones de analítica avanzada, siguiendo los criterios de Meldolesi et al. (2016). El Big Data proviene de una amplia variedad de fuentes, tales como ensayos clínicos, registros electrónicos de salud (EHR), registros y bases de datos de pacientes, datos multidimensionales del genoma, epigenómicas, transcriptómicas, proteómicas, metabolómicas, y las mediciones microbiomicas, y las imágenes médicas. Más recientemente los datos se están integrando a partir de medios de comunicación social, indicadores socioeconómicos o de comportamiento, información ocupacional, aplicaciones móviles, o a través del seguimiento del entorno, señalan Fernández-Luque y Bau (2015); el Big data viene en una amplia gama de formatos, y se hace necesario evaluar e interpretar los flujos de trabajo de una forma adecuada en el tiempo,

para beneficio de los pacientes afectados por enfermedades y a la vez ayudar a los ciudadanos que gozan de un buen estado de salud a conservarlo (Hood y Price, 2014).

Las complejidad del Big Data en materia de salud queda plasmada en la siguiente figura 2.0, a partir de las fuentes de los datos.

Figura 2.0.
Arquitectura conceptual aplicada de analítica del Big Data.



Fuente: Raghupathi y Raghupathi (2014)

Como recoge esta figura el Big Data en materia de salud puede provenir de registros internos de salud (por ejemplo, EHRs, registros de salud electrónicos, sistemas de apoyo a decisiones clínicas, CPOE -*computerized physician order entry*-, etcétera) y fuentes externas (fuentes gubernamentales, laboratorios, farmacias, compañías de seguros y HMOs –*health maintenance organizations*-, etcétera) con frecuencia en múltiples formatos (archivos planos, .csv, tablas relacionales, ASCII / texto, etcétera) y que además se encuentran en distintas ubicaciones (tanto geográficas como en diferentes sitios de proveedores de atención médica o sanitaria) en numerosas aplicaciones heredadas y otras (aplicaciones de procesamiento de transacciones, bases de datos, etc.).

El dato personal es hoy en día un bien económico (Moulia, Jean y Vilá Costa, 2016). Así las redes sociales son un campo potencial para obtener datos muy valiosos del usuario en relación a cualquier producto, marca, empresa, tendencias de consumo, comportamiento, conducta.

De acuerdo con Rincón (2016) los datos son "la cancha donde se juega la democracia". He creído necesario abordar el significado del Big Data, grandes datos o macrodatos (Aguilar, 2016) como paso previo al tratamiento de un derecho fundamental como es la protección de los datos de carácter personal; según Moreno (2014) se puede considerar una tendencia en el progreso de la tecnología que ha supuesto la apertura a un nuevo enfoque para la comprensión y la toma de decisiones, que es empleado para describir enormes cantidades de datos, información que de otro modo no se puede procesar o analizar utilizando herramientas o procesos típicamente tradicionales. Según este autor el desafío del Big Data consiste en capturar, almacenar, buscar, compartir y agregar valor a datos que hasta ahora se encontraban inutilizados o eran inaccesibles; por lo tanto lo relevanye aquí no es tanto el volumen de datos o su naturaleza, sino más bien su valor potencial, es decir, se trata de aportar y descubrir aquel conocimiento que está oculto, y hacerlo desde grandes volúmenes de datos. El Big Data implica una minería de datos para buscar correlaciones en los datos almacenados; el profesor Aluja (2001) ya utilizaba la definición de minería de datos avanzada por Hans (1998), entendida como un proceso de análisis secundario de grandes bases de datos con la finalidad de revelar relaciones desconocidas que pueden ser de interés o aportar valor al titular de una base de datos.

Auffray et al. (2016) abordan precisamente los beneficios que se pueden obtener del Big Data actualmente para la asistencia sanitaria; el Big Data en materia de salud se puede utilizar para mejorar la eficiencia y la eficacia de las estrategias de predicción y prevención o de las intervenciones médicas, de los servicios de salud, y las políticas de salud, entre otras funcionalidades. El acceso a datos relacionados con la salud de alta calidad tendrá probablemente una serie de beneficios en una variada gama de situaciones diferentes (Rumsfeld, Joynt y Maddox 2016; Bulger, Taylor y Schroeder, 2014).

En la práctica, el Big Data debe mejorar los resultados para los pacientes individualmente a través de la personalización de las predicciones, el diagnóstico temprano, unos mejores tratamientos, y la mejora en el apoyo a la toma de decisiones para los médicos en cada proceso clínico, como defienden Janke, Overbeek, Kocher y Lévy (2016) en su artículo cuyo nombre habla por si mismo *"exploring the potential of predictive analytics and big data in emergency care";* con la integración de la retroalimentación de una evaluación continua se completa este proceso. Estas mejoras deberían conducir a menores costes para el sistema sanitario.

De la misma manera, la integración de sistemas de información fragmentados en el ciclo de vida clínica permitirá el descubrimiento de asociaciones clínicamente relevantes, síntomas tempranos de una enfermedad, o cambios en el desarrollo de ciertas enfermedades y que, por lo tanto, permiten abordar mejores estrategias en la gestión de pacientes, así como mejorar la calidad y la seguridad de la atención. Abugessaisa et al. (2014) estiman que para los ensayos clínicos más amplios, los datos de salud

interoperables deberían facilitar la posibilidad de encontrar a los participantes adecuados y de diseñar y evaluar la viabilidad de nuevos estudios, como también defienden Cano et al. (2014).

El Big Data también ofrece ventajas en el ámbito de la farmacovigilancia pues una mejor gestión de grandes volúmenes de datos permitiría una identificación más sistemática de indícios que informen sobre la seguridad de los medicamentos, afirman Koutkias y Jaulent (2015), tales como la detección precoz de reacciones adversas a los fármacos, a la vez que facilita una medicina personalizada a través de los análisis de los pacientes y/o metodologías de estratificación de la población. Este escenario a su vez conduce a una mejora en la respuesta al tratamiento para subgrupos de pacientes biológicamente o clínicamente predefinidos, lo que también evita el rechazo innecesario de fármacos agresivos y dispositivos varios. El resultado de todo ello parece evidente, beneficios para los pacientes a la vez que la tendencia a un aumento de costes hospitalarios y de gestión de la atención sanitaria, así como los costes del diagnóstico y del desarrollo de fármacos por la industria biofarmaceútica se detiene o contiene. En todo caso, estoy de acuerdo con Auffray et al. sobre la necesidad de que especialistas en economías de la salud proporcionen **sistemas de medición adecuados para supervisar los "key performance indicators" (KPIs) o indicadores de rendimiento clave del éxito en los proyectos piloto de Big Data**.

Así, como reconoce Ohlhorst (2012) el Big Data y sus 4Vs abren el camino hacia la analítica de los datos, al proceso de aportar valor. Sin embargo, aunque la complejidad no termina con estas 4 dimensiones, sino que existen otros factores (un conjunto de tecnologías y sistemas analíticos) que se convierten en elementos factibles para su puesta en práctica que mueven el mundo de la empresa, por ejemplo; de esta manera, Ohlhorst cree que, aunque estos no son conceptos ni tecnologías del todo novedosos, sí deben incluirse bajo el paragüas del Big Data, a saber: (a)"*traditional business intelligence"* o inteligencia de negocios entendida como una categoría amplia de aplicaciones y tecnologías para recoger, almacenar, analizar y acceder a los datos, que aportan información para una mejor toma de decisiones; (b) *"data mining"* o minería de datos, es decir, el proceso por el que se analizan los datos desde distintos ángulos para extraer unos resultados que se consideran útiles, así pues se trata fundamentalmente de un proceso con fines predictivos y no tanto descriptivos; (c)"*statistical applications*" o el estudio de los datos a partir de algoritmos basados en principios estadísticos y normalmente se centran en un conjunto de datos censales o datos estáticos, y ofrecen muestras que pueden ser empleadas para el análisis predictivo; (d) *"predictive analysis"* que forma parte de las *"statistical applications"* resulta especialmente importante en el mundo científico y en el financiero donde conjuntos de datos se examinan para hacer predicciones a partir de tendencias e información extraída de bases de datos.

Pero se puede concluir que al final del camino lo importante no son los datos, ni siquiera la tecnología que se utilice para analizarlos, sino tener bien claro qué información necesitamos obtener de esos

datos y poder ser capaces de analizar correctamente los datos y de presentar los resultados de manera clara y concreta[53]; Si profundizamos un poco más en este análisis e incorporamos un valor espacial, mostrando los datos en un mapa, podemos hablar entonces del concepto de **geomarketing** (Yener, 2016; Nunes, Santana, Bezerra, y Sobral, 2014; Cliquet, 2013), que aporta el valor añadido que se requiere. La fusión del geoposicionamiento y el marketing dan lugar al geomarketing, que permite en primer lugar poder analizar, y más tarde sacar conclusiones, sobre un negocio o tipo de actividad, por ejemplo, de acuerdo a la localización de los consumidores o pacientes, a los puntos de atención o asistencia, a la competencia, etcétera. Desarrollar un proyecto combinado de *Business Intelligence*, Big Data y Geomarketing conduce a la posibilidad de poder analizar los datos y obtener resultados que contribuyan a una mejor toma de decisiones estratégicas, pero a la vez permite realizar predicciones sobre el futuro de un negocio, por ejemplo; como dijo Peter Drucker: **"La mejor forma de predecir el futuro, es crearlo"**[54]**.**

En cualquier caso, conviene recordar que el Big Data aplicado a la salud conlleva importantes implicaciones para la privacidad de los datos y la seguridad de la información, además de desafíos relativos a la calidad de los datos y su análisis, como bien apunta Hoffman (2016). Khan y Rehman (2017) previenen también del hecho que los datos pueden ser utilizados para manipular o predecir una próxima crisis de salud debido a cualquier desastre, virus o cambio climático, al mismo tiempo que la recopilación de datos de varias entidades relacionadas con la salud o de cualquier paciente plantea ciertas serias incertidumbres sobre la filtración, la integridad, la seguridad y la privacidad de los datos. Hablamos pues de los **riesgos ligados al uso del Big Data,** relativos a la protección de datos, la seguridad, la propiedad intelectual, o la privacidad (Ye et al., 2016; Chan y Moses, 2016; Van Staa, Goldacre, Buchan y Smeeth, 2016; Hilbert, 2016; Abbasi, Sarker y Chiang, 2016; Márquez y Lev, 2016; Blobel, López y González, 2016; Stylianou y Talias, 2016; Kenny, 2016; Raghupathi y Raghupathi, 2014; Crotty y Mostaghimi, 2014; Richards y King, 2014; Kitchin, 2013; Marx, 2013; Sagiroglu y Sinanc, 2013; Hamilton, 2013; Machanavajjhala y Reiter, 2012; Manyika et al., 2011). No en vano la realidad se vuelve transparente cuando se la somete al control, a la operatividad, al cálculo…en general, "cuando se allana" (Han, 2013)[55].

[53] Big Data y Geomarketing. Recuperado de http://www.mediapostgroup.es/blog/big-data-geomarketing-tandem-perfecto/. Último acceso el 25 de diciembre de 2016.

[54] Peter Drucker nació en Austria, trabajando en el mercado financiero y como periodista en Alemania, donde más tarde se doctoró en derecho. En 1937 escapó del nazismo y emigró a Londres primeramente y después a EE.UU., donde vivió como profesor universitario, consultor y escritor. Su primer libro de renombre fue "el concepto de la corporación" (1946), donde analiza General Motors desde su experiencia como consultor en la empresa que era entonces el símbolo de la gran corporación norteamericana. En 1954 publicó "la gerencia de empresas", base del management como nueva disciplina de gestión. Con 95 años murió en 2005, dejando ideas innovadoras que fusionan disciplinas como la economía, la sociología, la historia, la psicología...recogidas en numerosos artículos y libros, muchos traducidos al español; fue el más grande pensador del management del siglo XX, dijo de él Jack Welch, CEO de GE por aquel entonces, en un homenaje a quien consideraba su maestro. Un adelantado que dio forma a las organizaciones del siglo XXI; Drucker, P. (26 julio 2010). La mejor forma de predecir el futuro es crearlo. Recuperado de http://www.mercado.com.ar/notas/dossier/366011/1-peter-drucker-la-mejor-forma-de-predecir-el-futuro-e%3Cb%3Es%3Cb%3E-cr. Último acceso 25 diciemnbre 2016.

[55] Es lo que Vásquez Rocca (2015) llama " la sociedad de la transparencia y la hipervisibilidad de la era digital".

2.1.2. *eHealth*.

La Oganización Mundial de la Salud (OMS)[56] define la salud en su acta de consitución como un estado de completo bienestar físico, mental y social, y no solamente como la ausencia de afecciones o enfermedades[57], entiende el concepto de *eHealth* como el empleo de las ICT en el campo de la salud[58]. La OMS habla hoy en día de un ecosistema evolutivo de datos de salud a nivel mundial[59] que, en cada país y entre países, ofrece nuevas oportunidades en la atención sanitaria, para su práctica, la investigación y la detección. Se revela como un entorno con nuevas partes interesadas y nuevas capacidades como las tecnologías, donde los métodos analíticos y las políticas cambian y se adaptan, para así poder aprovechar el potencial del Big Data en el campo de la salud. Este entorno abre por lo tanto nuevas posibilidades y desafíos, y requiere respuestas innovadoras también. Más allá de las fuentes tradicionales de datos generados por las actividades de salud y salud pública, ahora se amplían las fuentes de datos, y surgen nuevas herramientas para capturar datos a través de sensores, *wearables* y monitores de todo tipo. Existen nuevos métodos analíticos que según la OMS nos permiten vincular datos diferentes, como son los del medio ambiente, geoespaciales, de estilos de vida y datos de comportamiento. Las nuevas capacidades tecnológicas permiten la generación, almacenamiento y explotación de datos a través de muy diversos aspectos de la salud humana (ver figura 2.1.). Así, los cambios en este ecosistema de datos de salud también se reflejan en la aparición de nuevos actores.

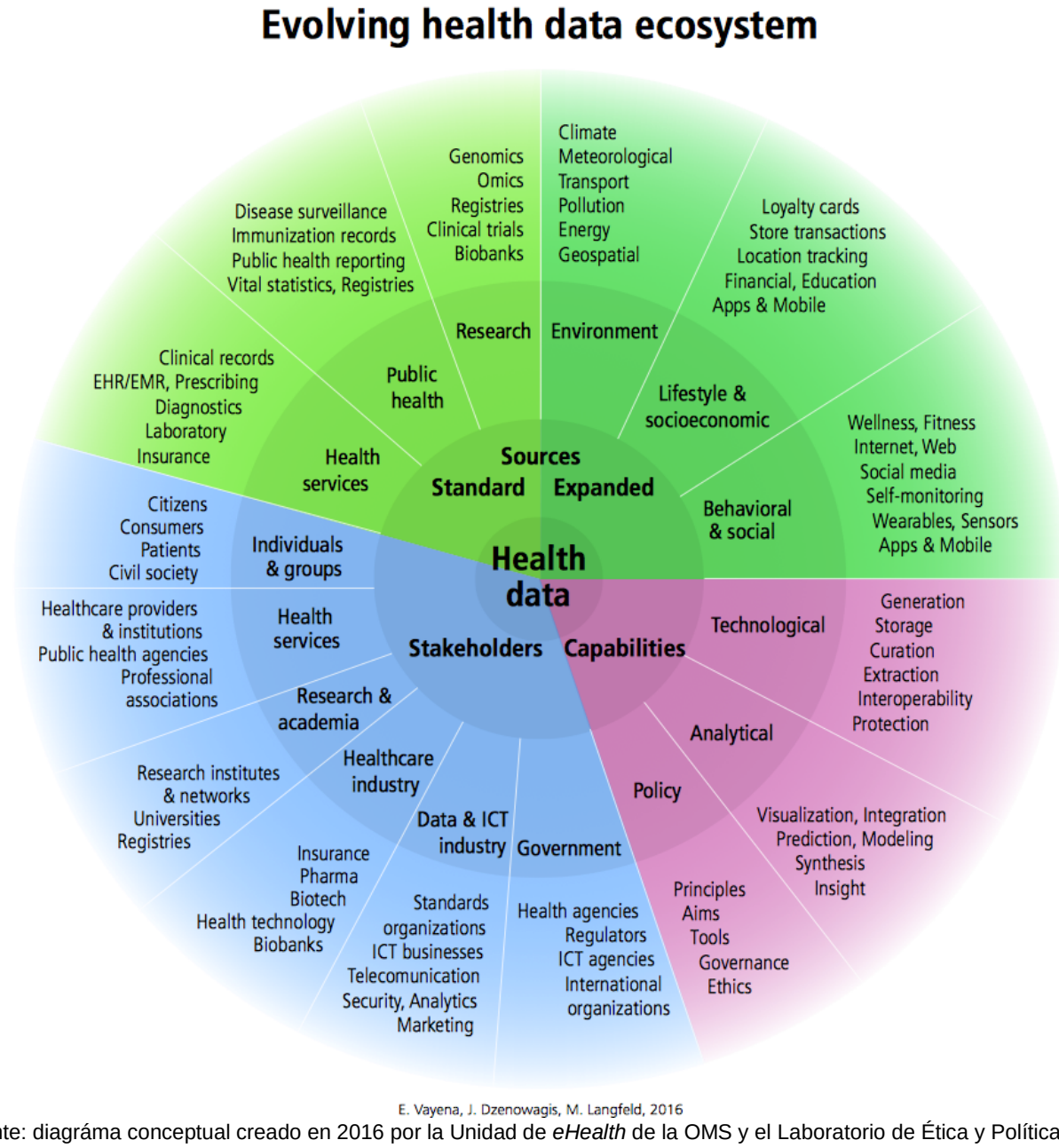
[56] La OMS es un organismo especializado de las Naciones Unidas (ONU) creado en 1948 cuyo objetivo es alcanzar, para todos los pueblos, el mayor grado de salud. Su papel y alcance ha sido discutido desde entonces y el debate se suele expresar en términos de si la organización es "apta para el propósito" aunque cuyo propósito no siempre es explicado. Ha habido varios intentos de reforma de la OMS desde su creación, encaminados a hacerla más apta para un propósito todavía controvertido. La actual ronda de la reforma de la OMS se puso en marcha en 2010 tras una crisis presupuestaria. El actual programa de reforma abarca la movilización de fondos, los presupuestos, la evaluación, las relaciones con los agentes no gubernamentales, las relaciones dentro de la secretaría (entre la sede, las regiones y las oficinas en cada país), el papel de la OMS en la gobernanza sanitaria mundial, el programa de emergencia y la gestión del personal de la OMS, temas que aborda en detalle Legge (2016).

[57] De acuerdo con la Representación de España ante Naciones Unidas y Organismos Internacionales. Recuperado de http://www.exteriores.gob.es/RepresentacionesPermanentes/OficinadelasNacionesUnidas/es/quees2/Paginas/Organismos%20Especializados/OMS.aspx. Último acceso 27 de diciembre de 2016.

[58] OMS. eHealth. Recuperado de http://www.who.int/topics/ehealth/en/. Último acceso 10 diciembre de 2016.

[59] OMS. The Health Data Ecosystem. Recuperado de http://www.who.int/ehealth/resources/ecosystem/en/. Último acceso 10 diciembre de 2016.

Figura 2.1.
Ecosistema de datos de salud.



Fuente: diagráma conceptual creado en 2016 por la Unidad de *eHealth* de la OMS y el Laboratorio de Ética y Políticas de Salud del Instituto de Bioestadística y Prevención de Epidemiología de la Universidad de Zúrich.

En cuanto al concepto genérico de *eHealth* he identificado múltiples definiciones, que tal vez se pueden reunir bajo el concepto de diseño, desarrollo, implementación y evaluación de las TIC en el sistema de salud, entendido de forma amplia; parece que existe un consenso, al menos en la UE, entendiendo que *eHealth* se refiere al uso y introducción de las tecnologías de la información y comunicación, a la vez que se refiere a un concepto interdisciplinario y que abarca múltiples instituciones (Moen, 2012).

El importante avance en materia de TIC, acompañado del creciente procesamiento de datos que ha conducido a un **acceso universal a la información**, ha tenido como consecuencia, entre otras, la globalización de todo tipo de servicios y todo tipo de negocios. En el sector de la salud esta tendencia se ilustra por una creciente consolidación del ámbito *eHealth*, un área donde confluyen la comunicación electrónica y la tecnología de la información para ceder, almacenar, y acceder a datos digitales con fines clínicos, educativos, y administrativos, tanto en la misma ubicación como en localizaciones distantes. Sin uso frecuente hasta prácticamente el año 2000[60], el concepto de *eHealth* se desarrolló para referirse a aplicaciones de salud en red (incluyendo todo lo relacionado con ordenadores y medicina); continuando así con la tendencia iniciada por el *eCommerce*, *eBusiness*, *eLearning*, etc[61]. El concepto *eHealth* fue aparentemente usado por primera vez por líderes del sector y profesionales del marketing antes que por el mundo académico[62].

Las soluciones de ICT basadas en Internet han demostrado tener capacidad para modificar la forma en que proveedores de salud, planes de salud, organizaciones, pagadores, reguladores, y consumidores acceden a la información, adquieren productos y servicios sanitarios, ofrecen cuidados, y se comunican entre ellos[63].

De acuerdo con algunos investigadores, el concepto telemedicina está vinculado a los profesionales de la medicina, mientras que el concepto de *eHealth* está impulsado por persones ajenas a la profesión, a saber los pacientes (consumidores); Allen (2000).

La esencia de *eHealth* (como en *eCommerce*) es una transacción fiable en un entorno cambiante que implica a personas, procesos, y una infraestructura empresarial dirigida al ciudadano enfermo o saludable. Se está estimulando una visión más amplia de *eHealth* como siguiente paso hacia un sector de salud en red; en países desarrollados *eHeatlh* ha evolucionado rápidamente desde la prestación de contenido sanitario en red hacia la adaptación de soluciones genéricas de eCommerce al procesamiento de transacciones administrativas relacionadas con la salud y al soporte logístico de tareas clínicas. Las aplicaciones de *eHealth* más emergentes están orientadas a las redes profesionales, la integración de gestión de procesos de cuidados clínicos, y la provisión de información de salud y cuidados del paciente a través de Internet, incluyendo asistencia sanitaria y monitorización remota.

[60] *eHealth* incluye muchos conceptos bajo el mismo paragüas y fue introducido como una solución a situaciones conflictivas como el tiempo de expera excesivo para los pacientes, la ausencia de acceso a la atención sanitaria, el elevado coste de prestación de los servicios y los errores médicos; Bliemel, M. & Hassanein, K. (2004).

[61] Mitchell (2000).

[62] Así lo recoge Eysenbach G. ya por el año 2001 en su artículo "What is e-health?" publicado en el Journal of Medical Internet Research.

[63] Della (2001).

Sprenger (2016) afirma que el término *eHealth* generalmente se refiere a actividades basadas en Internet, como la Web 2.0, en el contexto de la salud (Van Limburg et al., 2011), y recoge como Oh et al. (2005) realizaron una revisión de la literatura en la que identificaron patrones comunes en más de 50 definiciones del término e-health, como por ejemplo que (1) la salud *online* incluye tanto las actividades de salud como la tecnología, (2) que la tecnología es a la vez la herramienta habilitadora y la representación misma de la salud electrónica, o que (3) el *eHealth* a menudo implica distintas partes interesadas. Sprenger (2016) incide en los avances de la tecnología como motor de la existencia de una multitud de servicios de *eHealth* que se ofrecen actualmente, sin embargo apunta que la mayoría de estos servicios de *eHealth* resultan ser un fracaso, puesto que no se tiene en cuenta la viabilidad financiera, ni a los actores relevantes, ni el uso del servicio, ni muchas otras cuestiones de organización. Este es el punto en el que los modelos de negocio de los servicios de salud *online* pueden suponer una apoyo, ya que abarcan a todos los actores, así como sus interrelaciones para crear en común, entregar y capturar valor (Van Limburg et al., 2011).

De acuerdo con el proyecto epSOS de la Comisón Europea (que abordo extensamente en el apartado 3.4.3. referido a la interoperabilidad), el término salud electrónica o salud digital (*eHealth* en esta investigación) se refiere a herramientas y servicios de TIC destinados a la salud, empleados por profesionales de la salud, instituciones y administraciones así como a servicios públicos que proporcionan a los pacientes servicios relacionados con el cuidado de la salud de forma directa.

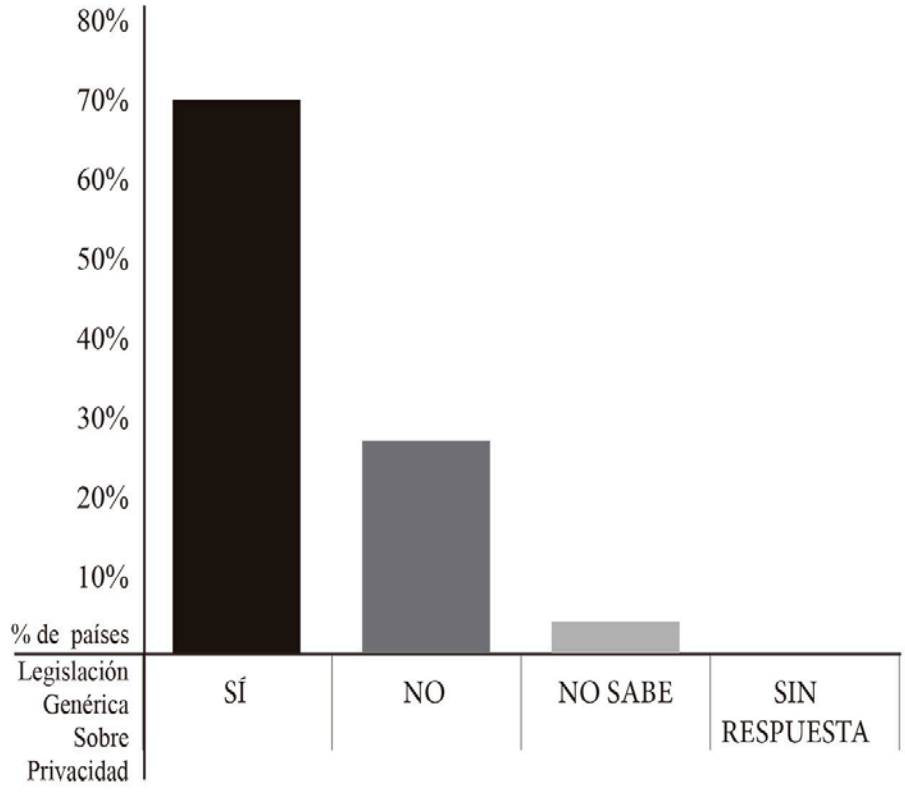
Navas Navarro (2015) describe el Big Data como "datos masivos", que considera datos digitales, y que en la actualidad pueden ser guardados en la nube; los responsables de los datos contratan servicios de computación para su almacenamiento y posterior tratamiento. La importancia del Big Data aquí radica en que el proveedor de estos servicios es el encargado del tratamiento, (que puede subcontratar con terceros a su vez). Al Big Data van unidos de forma intrínseca (en su ADN), por su especial protección, los datos de carácter personal.

Hay que tener en cuenta marcos jurídicos y éticos para el desarrollo del *eHealth*. Un mundo cada vez más conectado presenta enormes posibilidades en la manera en que trabajamos y vivimos, y en la naturaleza y calidad de los servicios que recibimos. Con estas oportunidades, sin embargo, vienen serios desafíos para que los datos de carácter personal y relacionados con la salud se mantengan seguros. La información de pacientes en formato digital puede ser objeto de abusos o errores. Muchos países están poniendo en práctica los marcos legales y éticos necesarios para asegurar que las personas y las comunidades de pacientes puedan sentirse seguras sabiendo que sus datos están bien protegidos. La segunda encuesta mundial sobre *eHealth* de la Organización Mundial de la Salud[64] fue diseñada para aprovechar la

[64] OMS. Survey 2009 Figures. Recuperado de http://www.who.int/goe/survey/2009/figures/en/index2.html. Último acceso el 10 diciembe de 2016.

base de conocimientos generada por la primera encuesta; si bien la primera encuesta fue general y se hicieron preguntas a nivel nacional, la segunda encuesta fue diseñada para ser temática con preguntas mucho más detalladas para explorar áreas específicas del *eHealth*. Los datos y análisis de la encuesta apoyan el fortalecimiento de las políticas de salud electrónica, la mejora de la protección ciudadana, la equidad de acceso y el multilingüismo, la promoción del crecimiento de la capacidad, herramientas y servicios de salud electrónica a nivel nacional y regional. Un total de ciento catorce Estados miembros optó por participar, y cómo refleja el gráfico 2.0. una importante mayoría (cercana al 70%) de los países que respondieron a la encuesta tiene vigente algún tipo de legislación sobre privacidad, y como señala Greenleaf (2015) el número de países que promulgan leyes de protección de datos continúa creciendo.

Gráfico 2.0.
Niveles mundiales de legislación genérica de privacidad.

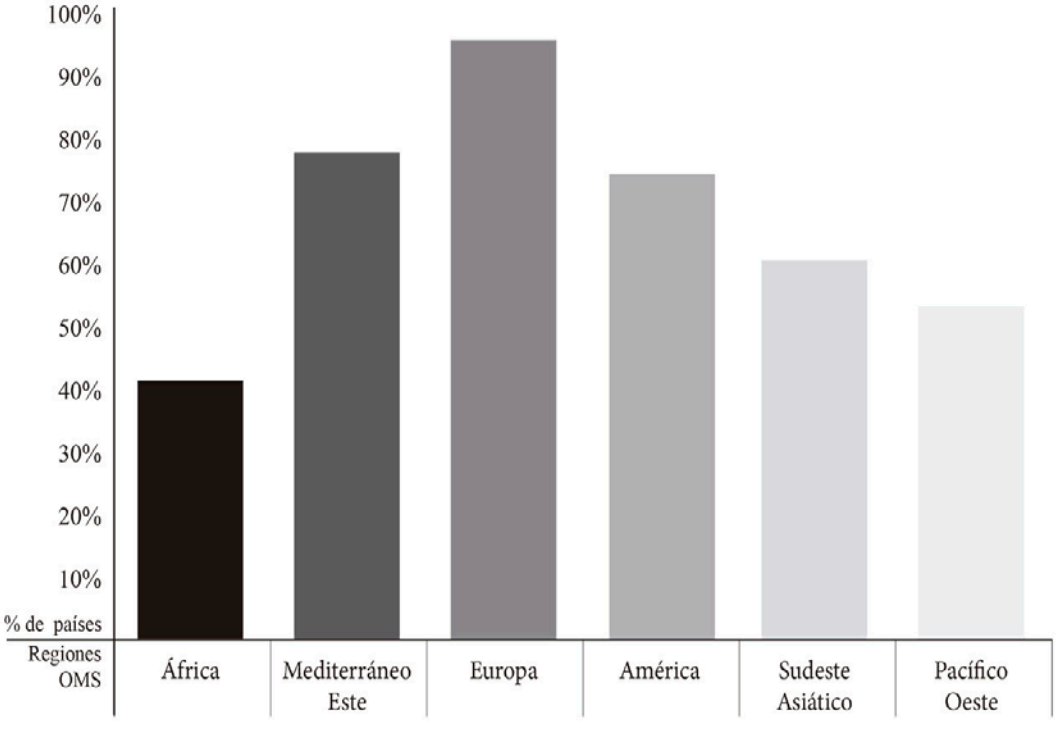


Fuente: gráfico de elabolación propia a partir de datos de la OMS

Es necesario señalar que el término “privacidad” tiene connotaciones muy diferentes por regiones del mundo; como señala la OMS en los países con ingresos más bajos la protección de la privacidad es más bien un lujo, puesto que adquieren preferencia otras necesidades más acuciantes. Así, los países de ingresos

bajos[65] disponen por lo general, en efecto, de un repertorio mucho menos sofisticado de derechos sobre la privacidad (incluidos los datos de salud), tal y cómo refleja el gráfico 2.1., en el que se puede comprobar que **Europa representa el mayor nivel de implantación de todas las regiones de la OMS.**

Gráfico 2.1.
Países con legislación genérica de privacidad establecida, por regiones de la OMS.

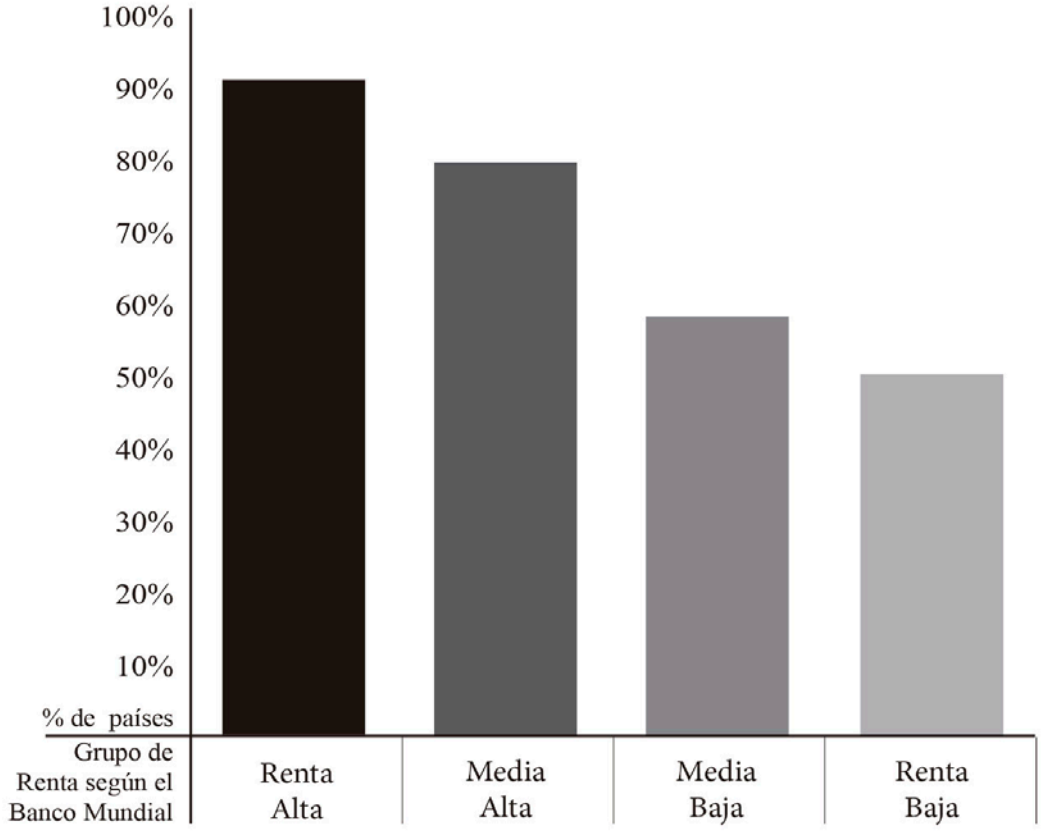


Fuente: gráfico de elabolación propia a partir de datos de la OMS

Si tomamos en cuenta los grupos de renta del Banco Mundial, un análisis pormenorizado del alcance de los datos de la OMS pone de manifiesto que generalmente es mayor el grado de prevalencia de la protección jurídica de la privacidad en países de renta elevada respecto a aquellos de renta más baja, como refleja el gráfico 2.2.

[65] OMS. Survey 2009 Figures. Recuperado de http://www.who.int/goe/survey/2009/figures/en/index2.html. Último acceso el 10 diciembe de 2016.

Gráfico 2.2.
Países con legislación genérica de privacidad establecida, por grupos de ingresos del Banco Mundial.



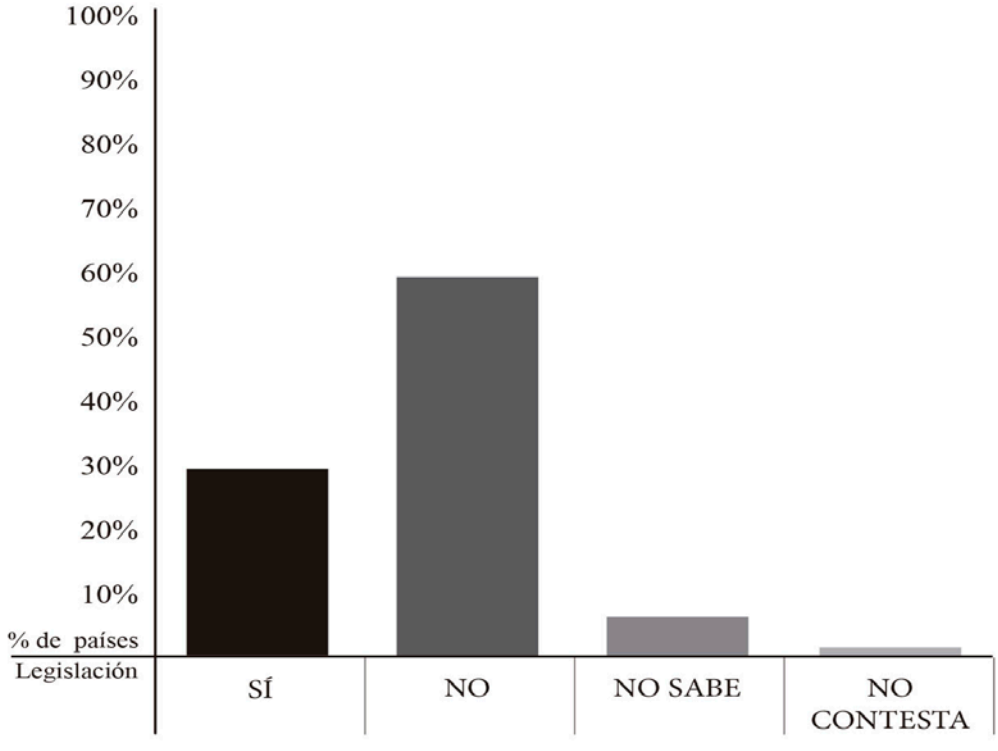
Fuente: gráfico de elabolación propia a partir de datos de la OMS

Resulta importante valorar si un impedimento a tener en cuenta a la hora de aplicar herramientas y soluciones de *eHealth* puede ser la falta de regulación de la privacidad, no ya desde el punto de vista de protección de los derechos humanos sino en qué medida el *eHealth* puede contribuir para fomentar la salud de los ciudadanos, especialmente si se tiene en cuenta el envejecimiento de la población (Dixon y Scheurell, 2016; Adamson, 2016; Kankanhalli, Hahn, Tan y Gao, 2016; Suzman, Beard, Boerma y Chatterji, 2015). De acuerdo con la OMS[66] son muchas las regiones, en especial Europa y América (junto al Mediterráneo Oriental), que ya han invertido numerosos recursos en soluciones de *eHealth* para dar respuesta al problema del envejecimiento de la población y están empezando a adoptar la idea de que, en este contexto actual de cambio demográfico, con el fin de satisfacer las necesidades de asistencia sanitaria será indispensable un cambio de paradigma en favor de una **atención de salud más centrada en el paciente y dispensada fuera del tradicional contexto del hospital o el consultorio del médico** generalista.

[66] OMS. Global Observatory for eHealth series (2012). Legal frameworks for eHealth.

Por otro lado, de las cifras de ámbito mundial del estudio de la OMS (ver gráfico 2.3.) se concluye que sólo cerca de un 28% de los países ha aprobado leyes que garantizan al paciente el acceso a su historia clínica electrónica, frente a un 63% que no lo ha hecho (un 8% contesta que "no sabe"). La promulgación de legislación relativa a HCEs otorga al paciente un cierto grado de control sobre sus datos de salud.

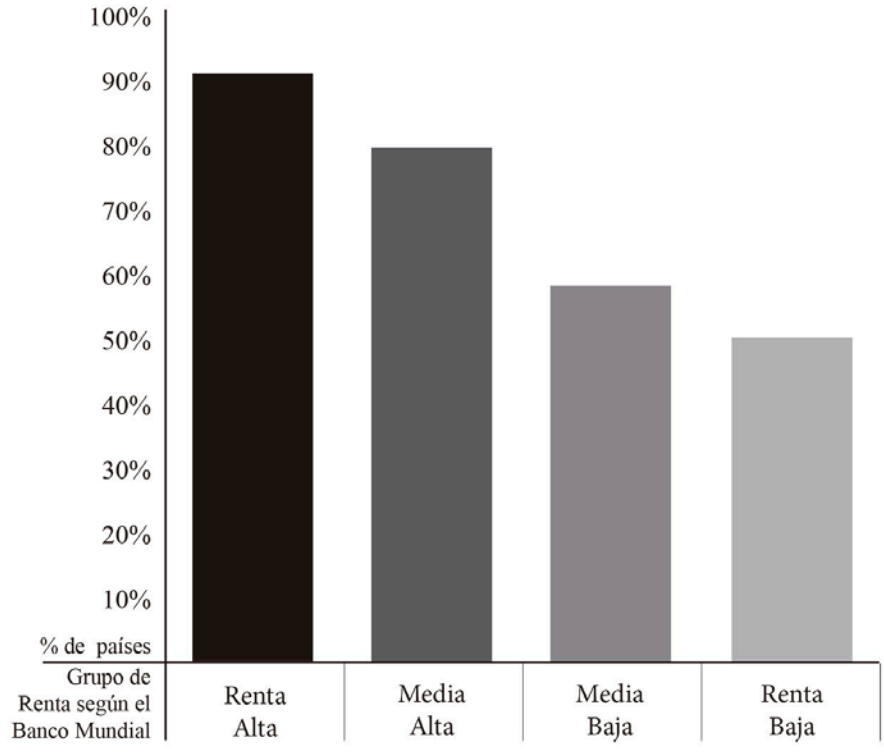
Gráfico 2.3.
Legislación establecida de protección de la privacidad de datos de salud digitales, a escala mundial.



Fuente: gráfico de elaboración propia a partir de datos de la OMS

Analizando los resultados de la OMS por grupo de ingresos del Banco Mundial y por región de la OMS (gráficos 2.4. y 2.5. respectivamente) se puede observar que todos los países de ingresos altos que confirmaron disponer de este tipo de regulación son miembros de la UE o del Área Económica Europea, hecho que puede atribuirse a la aprobación de la Directiva europea sobre protección de datos.

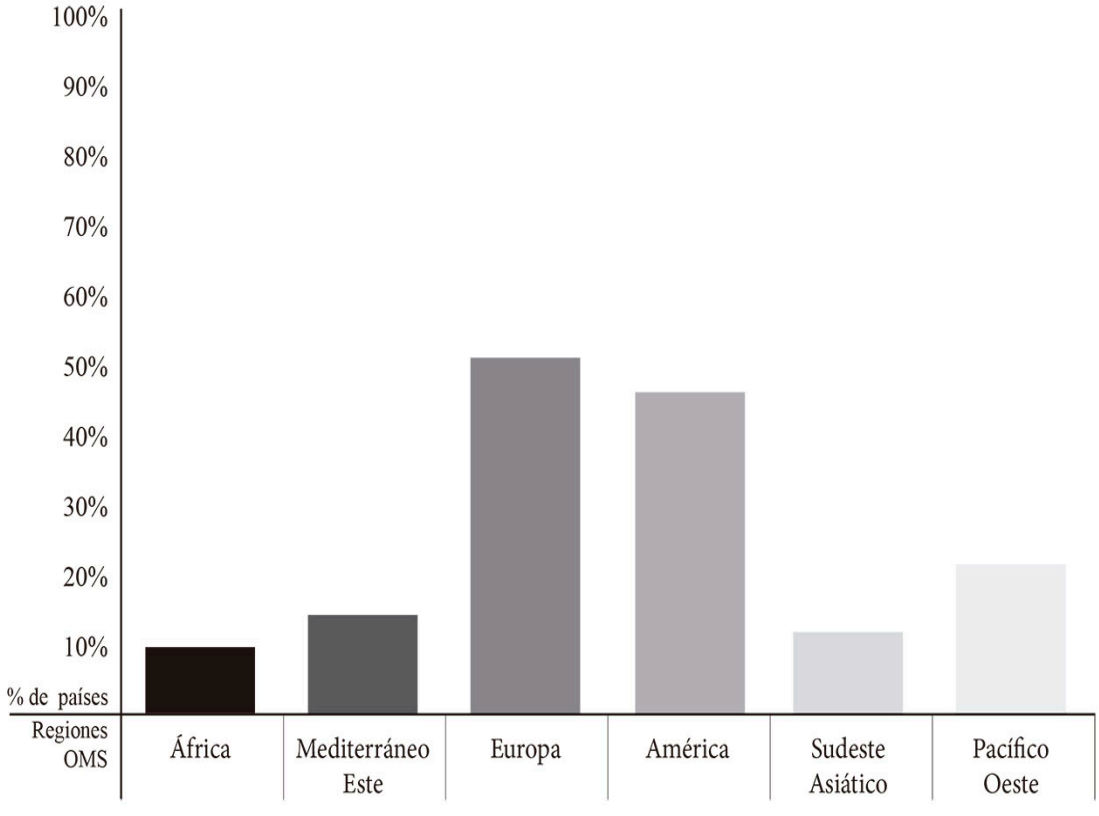
Gráfico 2.4.
Legislación establecida de protección de la privacidad de datos de salud digitales, por grupos de ingresos del Banco Mundial.



Fuente: gráfico de elaboración propia a partir de datos de la OMS

Al margen de los datos recogidos en los gráficos 2.4. y 2.5., la privacidad de los registros médicos queda protegida (no sólo por la ley sino) también por convenciones éticas y normas sociales, por lo que la OMS insiste en la relevancia de incorporar a **códigos deontológicos** nacionales (para el personal de salud) los imperativos básicos del juramento hipocrático, pues representan un instrumento fundamental para proteger los derechos de los pacientes. Especialmente por este motivo, en ausencia de una regulación específica sobre HCEs, los profesionales de la salud cuentan con un marco ético que debería ser adecuado para el uso de las nuevas herramientas (entorno *eHealth*).

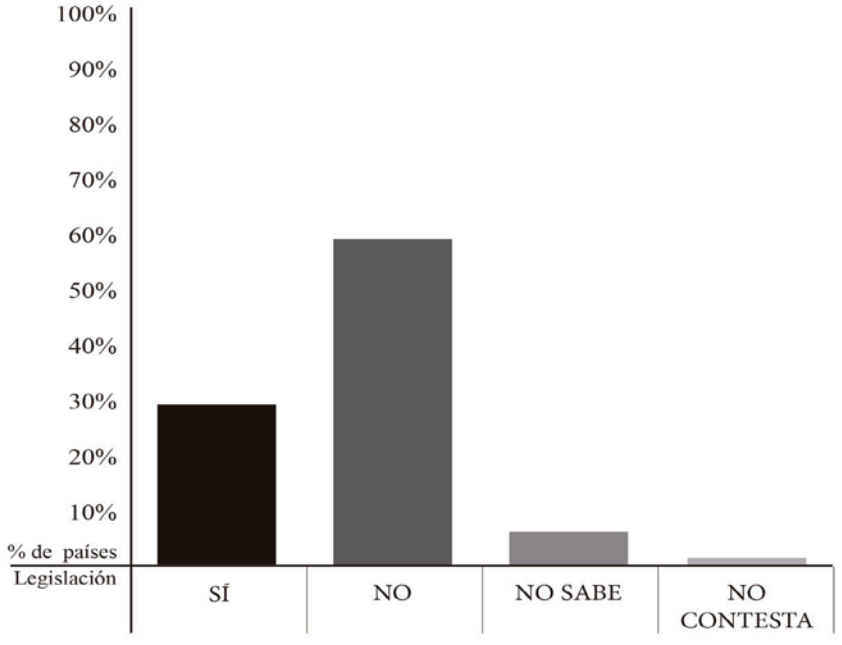
Gráfico 2.5.
Legislación establecida de protección de la privacidad de los datos de salud digitales, por regiones de la OMS.



Fuente: gráfico de elaboración propia a partir de datos de la OMS.

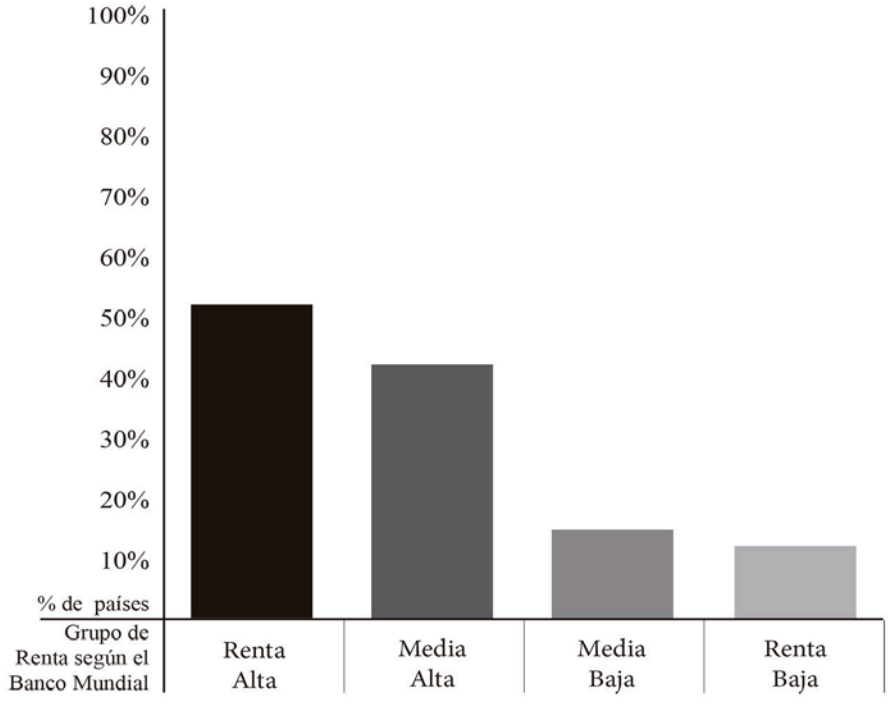
De acuerdo con los datos del estudio de la OMS (gráficos 2.6. a 2.9.) **a escala mundial no existe todavía una tendencia notable a aprobar una legislación específica que regule el intercambio de información entre profesionales sanitarios**; en el conjunto de respuestas obtenidas en todo el mundo, sólo uno de cada cuatro países afirmaba disponer de legislación de estas características. Por otro lado los países de ingresos altos de regiones como Europa y América destacan con una mayor tendencia a disponer de leyes que regulen el intercambio de datos entre profesionales sanitarios dentro de una misma institución y entre instituciones del mismo país.

Gráfico 2.6.
Legislación para compartir datos de salud (a través de la HCE) en las mismas instalaciones de salud, a escala mundial.



Fuente: gráfico de elaboración propia a partir de datos de la OMS.

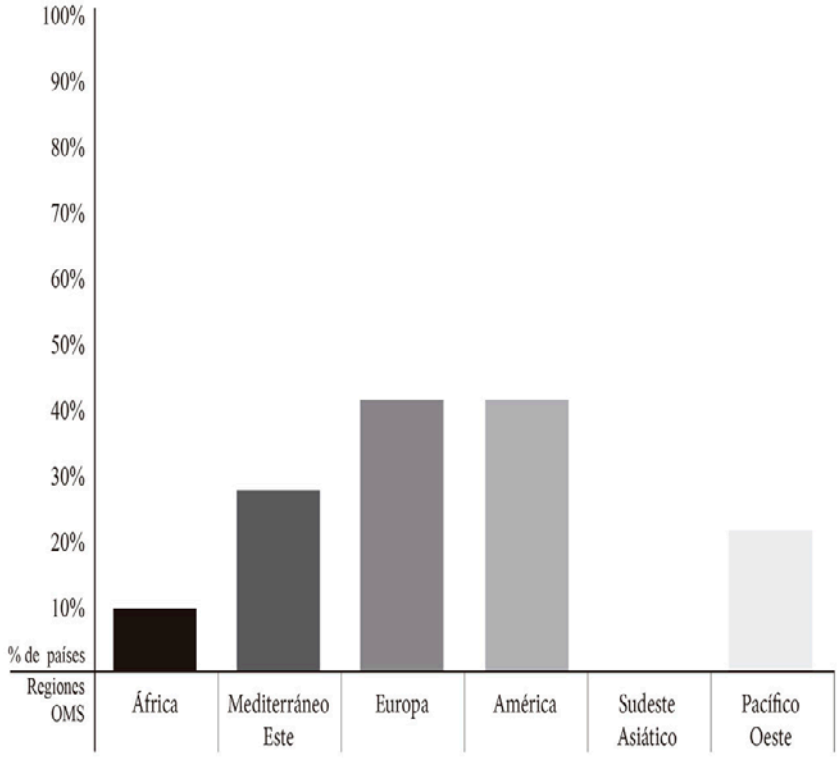
Gráfico 2.7.
Legislación para compartir datos de salud (a través del HCE) en las mismas instalaciones de salud, por el Banco Mundial.



Fuente: gráfico de elaboración propia a partir de la datos de la OMS.

Analizando los datos por región de la OMS y por grupo de ingresos del Banco Mundial, resulta digno de mención que en los países que ya han invertido significativos recursos en infraestructuras de *eHealth* y que informan de un nivel entre alto y medio de transferencias electrónicas de datos de pacientes, se observa precisamente un mayor madurez de este tipo de regulación sobre privacidad (gráficos 2.7. y 2.8.). **Se evidencia así el vínculo entre la ausencia o presencia de reglamentación sobre transferencias electrónicas de datos y el grado de madurez de las aplicaciones de *eHealth*;** se trata de la necesidad de adaptar los regímenes jurídicos pero también de que los principales representantes de los sistemas de salud interioricen (de acuerdo con el estudio de la OMS) las ventajas que, desde el punto de vista médico, se derivan del intercambio sistemático de los registros sanitarios electrónicos de pacientes, tanto dentro como entre los diferentes establecimientos de asistencia sanitaria. Los datos de la OMS revelan la directa correlación entre países que informan de un nivel muy alto, alto o medio de transmisión electrónica de datos (de pacientes en centros de salud locales) y los países que cuentan con legislación espefíca para regular esta transferencia.

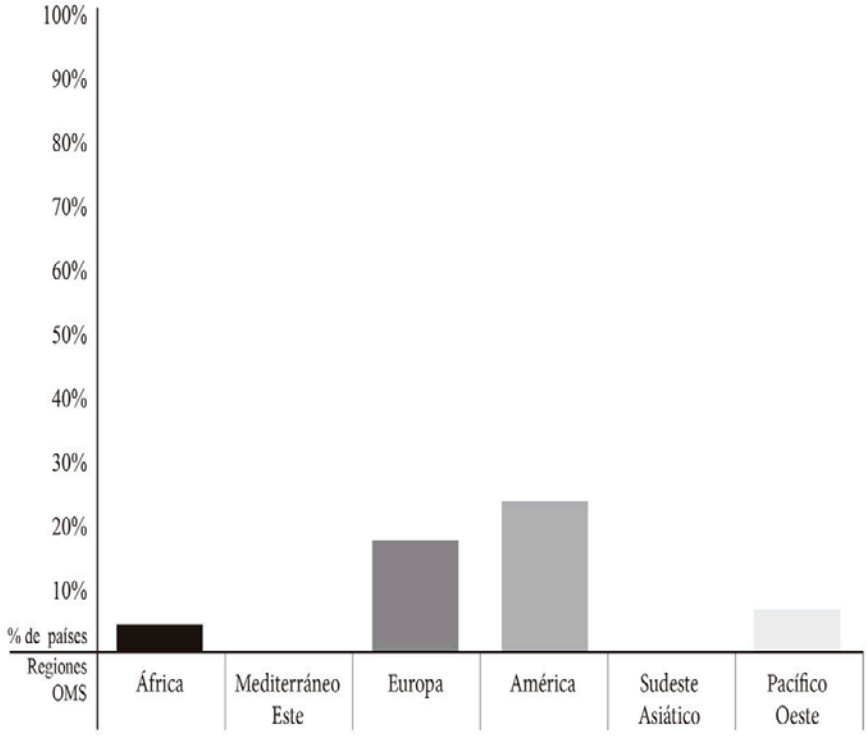
Gráfico 2.8.
Legislación para compartir datos de salud (a través de la HCE) en las mismas instalaciones de salud, por la OMS.



Fuente: figura de elaboración propia a partir de datos de la OMS.

Los datos de la OMS revelan no sólo dicha correlación directa entre nivel fluído de transmisión electrónica de datos y la existencia de legislación espefíca, sino que a la vez, ahora que tanto se habla del turismo sanitario y de la subcontratación transfronteriza de servicios médicos, no se ha avanzado demasiado en la regularización de la transferencia de datos, especialmente fuera de los países de ingresos altos; prácticamente sólo en Europa y América (gráfico 2.9.) se ha procedido a la regulación de dichas transferencias.

Gráfico 2.9.
Legislación para compartir HCEs con instalaciones de salud en terceros países, por regiones de la OMS.

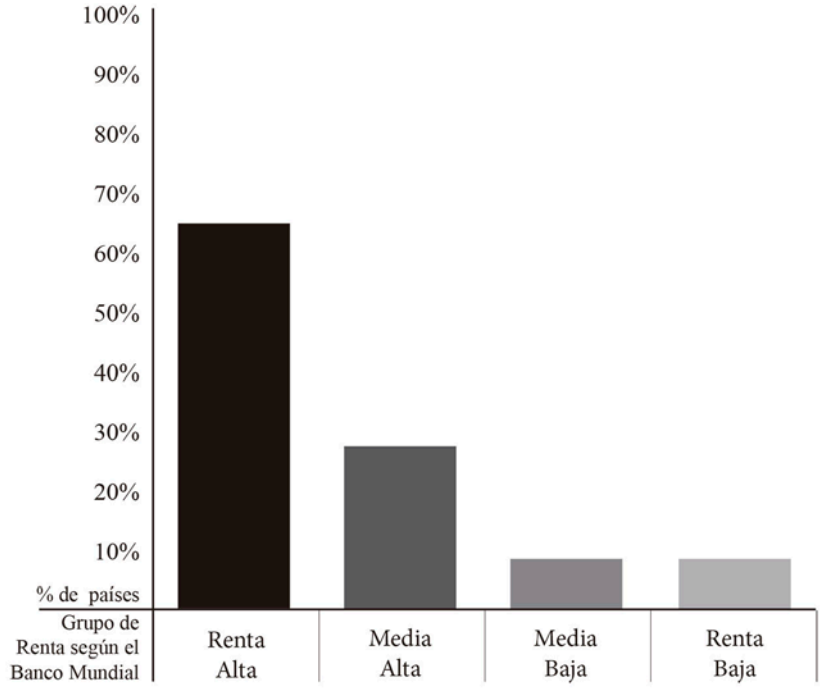


Fuente: gráfico de elaboración propia a partir de datos de la OMS.

Todavía existen pocas jurisdicciones que garanticen al paciente el derecho expreso a consultar su registro sanitario, aunque este dato coincide con el número de países que disponen de legislación en la que se trata explícitamente la privacidad de la HCE. Los países que ofrecen este tipo de derechos se encuentran ubicados de forma mayoritaria en el grupo de ingresos altos del Banco Mundial (gráfico 2.10.); los países con ingresos medio-bajos y bajos se quedan atrás en el reconocimiento de este derecho de los pacientes. El derecho de rectificación (gráfico 2.11.) coincide en general con el derecho de acceso, pero en pocas

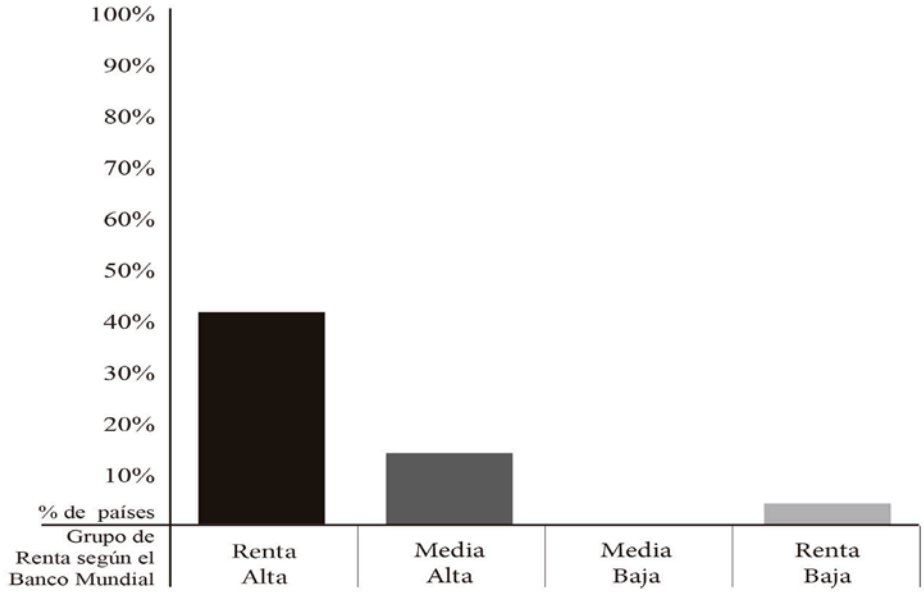
ocasiones y en contados países se admite el derecho a la supresión de los datos, y en tal caso se trata de supresión “dejando huella”.

Gráfico 2.10.
Legislación que garantiza a los individuos el derecho de acceso a sus HCEs, por grupos de ingresos del Banco Mundial.



Fuente: gráfico de elaboración propia a patir de datos de la OMS

Gráfico 2.11.
Legislaciones que reconocen el derecho de rectificación de los datos de salud de la HCE, por grupos de ingresos del Banco Mundial.



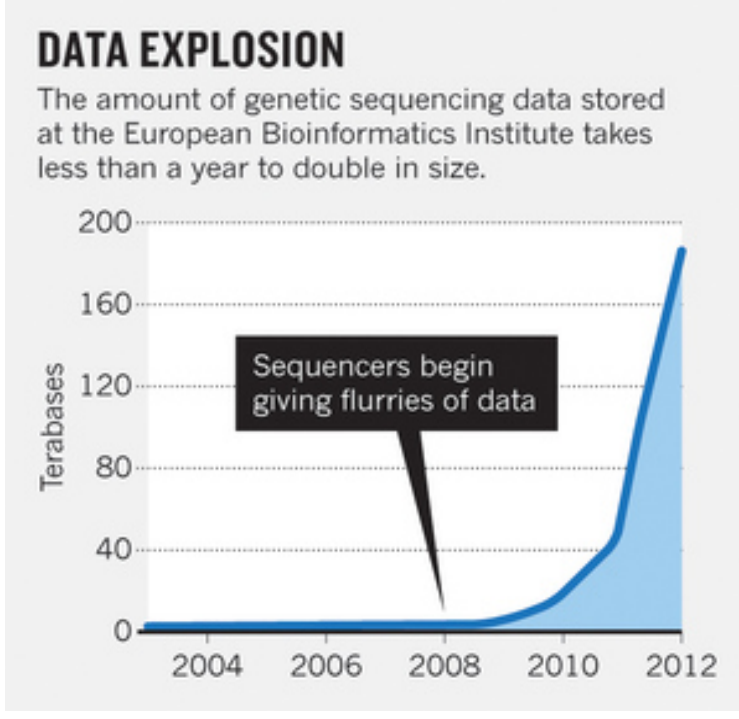
Fuente: gráfico de elaboración propia a partir de datos de la OMS

Se trata en conclusión, según la OMS, de generar confianza en las HCEs y optimizar su utilización para una más eficiente atención al paciente y con fines generales de salud pública. Algunos autores consideran al mHealth como parte del *eHealth*; la OMS estima que es un término emergente para definir la práctica médica y de la salud pública apoyado por dispositivos móviles, como teléfonos móviles, dispositivos de monitoreo de pacientes, asistentes personales digitales (PDAs) y otros dispositivos inalámbricos; aplicaciones de mHealth incluyen el uso de dispositivos móviles en la recopilación de datos de salud clínica o comunitaria, la prestación de información sanitaria a los profesionales, investigadores y pacientes, el seguimiento en tiempo real de los signos vitales del paciente, y la prestación directa de la atención sanitaria[67].

En cuanto a la explosión del Big Data y su crecimiente, el European Bioinformatics Institute (EBI) en Hinxton, Reino Unido, forma parte del European Molecular Biology Laboratory (EMBL) y emite informes científicos que muestran la evolución de los datos genómicos, como muestra el gráfico 2.12., y contribuye a entender el crecimiento exponencial de datos hoy almacenados, que tardan menos de un año en duplicar su tamaño.

[67] OMS. Survey 2009 Figures. Recuperado de http://www.who.int/goe/survey/2009/figures/en/index2.html. Último acceso 10 diciembe de 2016.

Gráfico 2.12.
Explosión de datos genómicos en el Instituto Europeo de Bioinformática.



Fuente: EMBL–EBI, 2013.

2.1.3. Protección de Datos.

2.1.3.1. Antecedentes históricos.

Históricamente en el Imperio Romano[68] hubo algún precedente de registro y control estatal de personas, pero se hacían censos sin periodicidad concreta, y consistía más bien en simples recuentos de ciudadanos, sin otra finalidad, aunque algun autor[69] mantiene la existencia de distintos tipos de censos en los que consignar datos como el nacimiento, la defunción y la ciudadanía de los romanos[70].

Los registros de datos de carácter personal comenzaron a generalizarse en Europa en el seno de la Iglesia Católica, a partir del Concilio de Trento celebrado en 1563, al pasar a regular la manera de llevar los

[68] El registro de sucesos vitales ya era conocido en el antigüo Egipto con fines propios de las administración pública, como la recaudación de impuestos, el servicio militar y el trabajo, a la vez que existen referencias de un registro de datos por parte de las autoridades civiles con similares fines en China (siglo X, A.C.), más tarde en Grecia (siglos IV y V, A.C.), y de forma más tardía en el Perú inca entre los años l,200 y 1,531 (Evolución histórica de los sistema de Registro Civil. Recuperado de http://www.monografias.com/trabajos16/evolucion-registro-civil/evolucion-registro-civil.shtml. Último acceso 12 diciembre de 2016).

[69] Schulz, F. (1946). History of Roman legal science.

[70] El Registro Civil. Recuperado de http://www.euskalnet.net/e-abizenak/verano02/c_genealogia.html. Último acceso 30 diciembre de 2016.

libros parroquiales de bautismos y matrimonios, como nos recuerda Gregorio (2004), pasando a incluir también los asientos de las defunciones. Este archivo o registro en cuestión sería implantado en España a través de la Real Cédula de 12 de julio de 1564 promulgada por Felipe II[71], extensiva a los territorios de ultramar, que en consecuencia **convierte a España posiblemente en el primer Estado moderno en crear y custodiar registros civiles[72]**, el antecedente de los registros civiles que se crearían a instancias estatales a partir del s. XIX -con una excepción: veinticinco siglos antes los judíos anotaban las genealogías de sus habitantes en registros cuya custodia se llevaba a cabo probablemente en el Templo de Jerusalén, y hay muchos indicios en el Antiguo Testamento donde se encuentran numerosos árboles genealógicos, y el propio Evangelio muestra dos genealogías completas de su personaje central, que ofrecen Lucas (Lc. 3, 23-38) y Mateo (Mt. 1, 1-17)-.

Finalmente (dada la relevancia de estos datos para el Estado) las autoridades civiles en distintos países europeos tomaron la decisión de crear los registros civiles, movimiento que se vió impulsado por la Revolución Francesa que tuvo como consecuencia la separación entre el Estado y la Iglesia. En España, por ejemplo, el Registro Civil se crea en 1870 y comienza a operar el 1 de enero de 1871, entrando España en una etapa moderna (en cuanto a los valores estadísticos y su relevancia para estudios demográficos); sin embargo, como indica Escandell (1986), hay que matizar este dato debido a los precedentes del registro civil en España, pues posiblemente el precedente más antiguo del interés del Estado por esta materia es la Real Cédula del 21 de marzo de 1749, bajo el reinado de Fernando VI, que encarga a los eclesiásticos que los libros de bautismo, casamientos y entierros se custodien en las mismas iglesias de modo seguro. En todo caso la implantación efectiva del registro civil en nuestro país se produce a lo largo del siglo XIX y de acuerdo con Escandell las "principales disposiciones que lo desarrollan fueron promulgadas en las etapas políticamente innovadoras -liberales, progresistas, demócratas- que intentaron bien modernizar las bases del Estado; bien desplazar a la Iglesia Católica del control sobre la existencia de los ciudadanos"; hasta 1840 no se experimenta ninguna tentativa seria que reemplace al registro eclesiástico, pues las disposiciones se limitan a trasladar datos parroquiales a los ayuntamientos, y el Decreto del 24 de enero de 1841 es el único precedente importante (sin que la Ley Provisional de 1870 aportase innovación real) aunque la subordinación al registro eclesiástico hicieron fracasar las intenciones de crear un registro civil de carácter administrativo. Así, en última instancia fue la Ley Provisional de Registro Civil de 1870 la que impone el traslado de las inscripciones de nacimientos, defunciones y matrimonios de los ayuntamientos a los juzgados, quedando de esta manera al margen de los registros parroquiales de forma definitiva.

[71] Del Registro Civil más antigüo que se conoce: el del Templo de Jerusalén. Recuperado de http://www.mundoarchivistico.com/?menu=articulos&id=477. Último acceso 10 diciembre 2016.

[72] En España el Cardenal Jímenez de Cisneros, Arzobispo de Toledo, ya había ordenado en el siglo XV la introducción de registros bautismales en todas las parroquias para evitar conflictos futuros como eran los matrimoniales. En Inglaterra se pidió a los Clérigos que registraran los bautismos, bodas, entierros por orden de Thomas Cromwell, Vicario General en época de Enrique VIII. En Francia el Registro Civil se introdujo en el siglo XVI cuando Francisco I promulgó la ordenanza Villers-Cotterets por la que se prescribía que los párrocos quedaban obligados a mantener registros de bautismos y entierros de aquellas personas que residían en los límites de la párroquia (Evolución histórica de los sistema de Registro Civil. Recuperado de http://www.monografias.com/trabajos16/evolucion-registro-civil/evolucion-registro-civil.shtml. Último acceso 12 diciembre de 2016).

Es interesante tener en cuenta la evolución de los registros desde el siglo XIX hasta hoy. De tal manera que el mantenimiento de registros con datos de carácter personal ha cobrado relevancia, no tanto desde el punto de vista de la laicidad del Estado, sino de la confidencialidad de la información y la protección de los datos de esta índole. Como destaca Domínguez (2016) conviene recordar la finalidad que justifica la existencia de un registro obligatorio, especialmente cuando aporta información a la administración sanitaria sobre la incidencia y/o evolución de una enfermedad como el VIH; en su opinión, muy acertada a mi entender, la implantación de la HCE (aspecto que abordo en detalle en el apartado 2.1.6.) ofrece muchas ventajas desde el punto de vista sanitario pero también desde el punto de vista de las libertades individuales, pues elimina la existencia de cualquier registro obligatorio de portadores de VIH, y la discriminación a la que puede conducir en muchas actividades de la vida cotidiana. Hace ya casi 30 años defendía Rigaux (1990) que las modernas técnicas de penetración en las aptitudes individuales o el comportamiento individual tienen hoy el respaldo de los métodos informáticos que establecen interconexiones entre características y comportamientos a los que se les confiere una apariencia de rigor científico, cuando las conclusiones resultan por lo general discriminatorias pues "en la creencia de descubrir en el sujeto ciertos signos anunciadores de su comportamiento futuro, el perfil instaura una forma de determinismo incompatible con el atributo más preciado de la libertad, la elección de un futuro autodeterminado". Es lo que Domínguez identifica con evidentes efectos perjudiciales, cuando la identidad y **los datos de carácter personal de un ciudadano se incorporan a las llamadas listas negras**[73] que la propia Comisión Europea, de una forma genérica señala: "consistiría en la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación". La Comisión entiende que este es un fenómeno amplio y de distinta índole y contenido (desde datos relativos a la salud o informaciones genéticas, a listados de morosos o de infracciones criminales o administrativas, de índole laboral, de carácter ideológico o sobre comportamientos políticos, sobre índices de peligrosidad de los individuos, ficheros sobre conductas consideradas inadecuadas por determinados sectores sociales, sobre datos adversos de los candidatos a un puesto de trabajo, etcétera). Las autoridades de control en distintos países de la UE han podido verificar la existencia de **ficheros de esta índole que son creados y gestionados de forma privada** y hacen referencia principalmente a ficheros existentes en grandes superficies o en compañías de alquiler de vehículos, referido a la comisión de infracciones penales; se trataría de la recogida y tratamiento de datos de carácter personal de "clientes indeseables" (que se podrían extender a otro tipo de clasificaciones en función de determinadas características o situaciones personales de

[73] Documento de trabajo sobre las listas negras. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_es.pdf. Último acceso 3 noviembre de 2016.

los individuos). Las autoridades de control han solicitado a los responsables de los ficheros la necesidad de acabar con estas prácticas, no siendo admisible la existencia de este tipo de ficheros en manos de compañías privadas. Para poder existir legalmente, deben cumplir con los principios de legitimación (artículo 7 de la Directiva 95/467CE), y en cualquier caso, el tratamiento de datos debe siempre respetar los principios de calidad de datos de acuerdo con la Directiva 95/46/CE.

Más aún, en el caso de que las listas negras incluyan datos especialmente protegidos, como los de salud, algo que ocurre a menudo respecto a seguros de vida, su recogida y difusión queda regulada por los arts. 8, 13 y 15 de la Directiva 95/46/CE; salvo que exista una regulación legal específica que estipule las garantías necesarias, sólo se podrán mantener dichos registros con el consentimiento libre, específico, explícito e informado del interesado (que lo podrá revocar en cualquier momento) y siempre de acuerdo al artículo 6 de la Directiva 95/46/CE, especialmente en cuanto se refiere a la proporcionalidad, creación de dichos ficheros en relación a los fines establecidos. En relación con esta clase de listas negras alguna autoridad de control nacional se ha opuesto a la existencia de ficheros centralizados por una federación de aseguradoras, en donde se incluían datos de personas a las que se había impedido la contratación de seguros de vida por razón de su estado de salud.

En todo caso, para alcanzar la máxima **armonización en materia de listas negras**, convendría eliminar los criterios divergentes que existen entre los Estados miembros, en línea con la Directiva 95/46/CE[74].

Un derecho básico que otorga la Directiva 95/46/CE consiste en la obligación de que los ciudadanos sean informados acerca del tratamiento de sus datos de carácter personal (es la también denominada notificación al interesado); el incumplimiento de este principio conduciría a su absoluta indefensión, pues no podrán tener conocimiento de la inclusión de sus datos de carácter personal en una lista negra, al no recabarse de ellos la información, y quedarían así privados del ejercicio efectivo de sus derechos de acceso, rectificación, cancelación y oposición[75]. Así exige una clara indicación de las condiciones, en su caso, para que pueda realizarse la comunicación de los datos a terceros[76].

[74] Considerando 7 de la Directiva 95/46/CE: *"Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales , reglamentarias y administrativas de los Estados miembros"*.

[75] Artículo 11 Directiva 95/46/CE: "*información cuando los datos no han sido recabados del propio interesado: 1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: las categorías de los datos de que se trate; los destinatarios o las categorías de destinatarios de los datos; la existencia de derechos de acceso y rectificación de los datos que le conciernen, todo ello en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal*

La Directiva 95/46/CE aborda la articulación de mecanismos que incluyan la información que se facilita al interesado al denegársele un servicio determinado y, en su caso, prevé la posibilidad de comprobación y verificación posteriores por su parte; se reconoce el derecho del afectado a no sufrir una decisión con efectos jurídicos que le afecte de manera significativa y que esté basada únicamente en un tratamiento automatizado de datos destinados a evaluar aspectos de su personalidad[77].

Sin olvidar que en el caso de ficheros centralizados, comunes y compartidos, es el del establecimiento y aplicación de las medidas de seguridad técnicas y de organización adecuadas, así como las condiciones de acceso a los mismos, obligaciones que recaen en el responsable del tratamiento[78]. Puesto que hay un número de sectores importante (sector sanitario, financiero o de telecomunicaciones) en los que este tipo de ficheros que incluyen listas negras afecta a un gran número de ciudadanos, la propia Comisión[79] ha querido concienciar sobre el tratamiento de datos de carácter personal y destacar la necesidad de que en este contexto existan criterios comunes, algo que el nuevo RGPD debe superar.

Al margen de los registros en las listas negras, Gregorio (2004) incide en el hecho de que ya en 1948 la Declaración Universal de Derechos Humanos recoge expresiones muy claras (artículo 12): "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". Como recuerda Mañas (2009) existen unos derechos fundamentales que constituyen la base de cualquier sociedad democrática avanzada, y que él identifica con la protección de datos, la seguridad y la transparencia; el respeto al derecho a la protección de datos ya se recoge en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), que en su artículo 8 reconoce expresamente el derecho a la protección de datos de carácter personal, que por otro lado, recoge el artículo 18.4 la Constitución Española (CE). El derecho a la protección de datos está ampliamente reconocido en sociedades avanzadas como la europea, en el marco de la UE, en los Estados miembros (España entre ellos) y, como afirma Mañas, España "posee una de las legislaciones más garantistas y uno de los sistemas de tutela más eficaces".

---

respecto del interesado. 2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas".

[76] Apartado 1 del artículo 11 de la Directiva 95/46/CE.

[77] Artículo 15 de la Directiva 95/46/CE relativo a "Decisiones individuales automatizadas".

[78] Artículo 17 de la Directiva 95/46/CE relativo a "Seguridad del tratamiento".

[79] Documento de trabajo sobre las listas negras. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_es.pdf. Último acceso 3 noviembre de 2016.

El derecho fundamental a la protección de datos es un **derecho autónomo e independiente** del derecho a la intimidad o del derecho al secreto de las comunicaciones privadas[80], y representa *de facto* uno de los aspectos más novedosos y controvertidos en la sociedad actual, especialmente en tiempos del Big Data; interferencias en el ámbito individual de las personas que surgen de la incorporación de datos de carácter personal a bases de datos en las que se nos identifica de forma directa o indirecta en relación con situaciones o hechos determinados.

Respecto a la jurisprudencia y el concepto de protección de datos, la corte de Estrasburgo (Tribunal Europeo de Derechos Humanos) ha ido más lejos que los demás órganos del Consejo de Europa[81], y así se deriva de los dos principios básicos que ha señalado: (1) la protección de datos de carácter personal forma parte del derecho al respeto a la vida privada (desautorizando así al Comité de Ministros que dio la respuesta contraria a la Asamblea Consultiva) y (2) en la regulación de ese derecho los Estados gozan de un amplio margen de apreciación (Miguel 2003); así pues queda patente que en Europa (y no sólo en la UE) el derecho a **la protección de los datos de carácter personal aparece directamente conectado con el derecho al respeto de la vida privada, pero va más allá del concepto de "privacy";** hay una tendencia a pensar que son derechos equivalentes pero la diferencia entre los dos en la Carta de Derechos Fundamentales de la UE no es puramente simbólica.

García y De los Ángeles (2013) abarcan el origen y la evolución del derecho a la protección de los datos de carácter personal a partir del derecho a la privacidad, reconocido en los distintos instrumentos internacionales del siglo XX, pero lo distinguen de otros conceptos como la intimidad, aunque ha contribuido a su promoción constitucional como derecho fundamental. Se trata pues de reciente derecho fundamental (nuevo o inexistente en muchos países), de origen europeo e importado en la realidad actual por otros países. Se trata pues de una materia que abarca desde el Derecho Constitucional y el Derecho Internacional Público al Derecho Internacional Privado, ramas muy enriquecedores para entender en conjunto los derechos de carácter personal, muy de utilidad en el análisis de las tendencias actuales del Derecho, en tiempos del Big Data e Internet que tan frecuentement colisionan con la intimidad.

Como recuerda Mañas (2009) existe un Derecho de oposición de la persona, en la utilización de las nuevas tecnologías para contribuir al respeto del derecho a la intimidad; el derecho a la protección de datos concede a su titular el poder de disposición sobre sus propios datos personales, pues se erige como un derecho autónomo e independiente del derecho a la intimidad.

[80] Documento de trabajo sobre las listas negras. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_es.pdf. Último acceso 3 noviembre de 2016.

[81] El Consejo de Europa está formado hoy por 47 países miembros, incluidos los 28 Estados miembros de la UE, compartiendo valores y principios, como recoge http://www.coe.int/en/web/portal/european-union. Último acceso el 3 enero 2017.

Como bien señalan García y De los Ángeles (2013) el derecho a la protección de datos también puede conflictuar con otros derechos fundamentales como son: la dignidad, privacidad, propia imagen, honor, vida, información; creen "que habrá de resolverse atendiendo a cada caso y recurriendo a la técnica de la ponderación de derechos". En la situación actual la sociedad se enfrenta a cambios estructurales importantes que van de la mano de la globalización y las nuevas tecnologías; un contexto que relaciona a todos los individuos entre sí, en función de diversos roles, así la información que surge en estas interacciones debe salvaguardar los derechos de la persona, como son la privacidad y la protección de datos de carácter personal.

Así, nos encontramos ante nuevos retos en lo que se ha llamado sociedad de control (Rodríguez, 2016; Alcántara, 2008; Deleuze, 2006), resultado de la continua injerencia de las TIC en nuestras actividades cotidianas, herramientas empleadas por necesidad en algunos casos, y siempre bajo la sombra de la vigilancia, por distintas razones e intereses, como apunta Garriga Domínguez (2016).

2.1.3.2. Dato de carácter personal.

La propia Directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995, referida a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal y a la libre circulación de estos datos, lo define (en su artículo 2 letra a) como "*toda información sobre una persona física identificada o identificable"*, que puede ser relativa tanto a su identidad física, fisiológica, psíquica, económica, cultural o social; esta definición es recogida por el artículo 3 letra a de la LOPD y detallada en el artículo 5 letra f del Reglamento de desarrollo de la LOPD (RLOPD)[82] en el siguiente sentido: *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*. En el concepto de dato de carácter personal se debe entender el significado de la palabra "información" en el sentido más amplio, **incorporando en su ADN toda clase de afirmaciones sobre una persona**, bien sea información "objetiva" (como por ejemplo, los datos sobre su salud) como "subjetiva" (cualquier opinión o evaluación sobre su fiabilidad, por ejemplo, como parte contratante). Para que sea aplicable el derecho a la protección no es preciso que la información esté probada o sea verídica. La información comprende también los denominados datos sensibles (artículo 8 Directiva 95/46/CE), que incluye la información referida a la vida personal y familiar de la persona, como a su actividad laboral, económica o social; esta información comprende cualquier tipo de formato o soporte, así pues puede considerarse dato de carácter personal cualquier información alfanumérica, gráfica, fotográfica o sonora.

[82] Real Decreto 1720/2007.

La **creación de conocimiento** tiene lugar en y entre personas, como recuerda Domínguez (2016), de la misma manera que se ubican datos en registros e información en mensajes, y de esta manera se puede obtener conocimiento de individuos o grupos de individuos.

De acuerdo con el artículo 2 del RLOPD, en la LOPD queda excluido el tratamiento de datos relativo a personas jurídicas (o a personas físicas que presten sus servicios en aquellas), a empresarios individuales, o personas fallecidas.

2.1.3.3. Dato de salud.

En general en el ámbito de la salud, de acuerdo con Sanz (2016), hay un solapamiento en cuanto al origen de los datos, y todos ellos pueden tener interés (en el ámbito sanitario) en función de la aplicación de los algoritmos que su utilizen para su análisis; unos proceden de la asistencia médica, otros de la investigación, otros del área de la salud pública, o del ámbito administrativo, o simplemente son incorporados como consecuencia del registro de actividades sociales.

Como datos sensibles[83] que son, llevan en su ADN todas las facetas de nuestra vida que afectan al bienestar y calidad de vida, como el número de pasos que damos al día, las calorías que quemamos, nuestra alimentación y dieta, las horas de sueño o el ejercicio diario. Actualmente existen infinidad de aplicaciones que recopilan información sobre nuestra salud y todas sus facetas. Dispositivos como los smartphones, y muy especialmente los wearables, disponen de tecnologías destinadas para evaluar o medir aspectos que afectan a nuestro bienestar como por ejemplo el lector de ritmo cardiaco que ofrecen los Galaxy S5 o Gear S84.

Alguna redes sociales, en algunos casos reconocen, el valor del dato de salud: "we the people…have the right to our own health data."; así lo ha declaraba en 2009 Patients Like Me que ha reconocido la Declaración de Derechos de Datos de Salud[85] contenida en www.healthdatarights.org (página hoy inactiva

[83] La LOPD califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, y establece un régimen especialmente riguroso para su obtención, custodia y eventual cesión, como recogería más tarde 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 defensa de la confidencialidad que había sido consagrada por la Directiva 95/46/CE), en la que *"además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada individuo, como destinatario por excelencia de la información relativa a la salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general"*.

[84] Belt.es. Los datos de tu salud que recopilan los dispositivos, un negocio para las empresas. Recuperado de http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=18211. Último acceso 10 diciembre de 2016.

[85] Recuperado de http://blog.patientslikeme.com/2009/06/22/patients_like_me_declare/. Último acceso el 25 de octubre de 2016.

desgraciadamente), lo que supone un reconocimiento por parte de empresas privadas (en la era del Big Data) de los derechos sobre los datos de salud, en una época en que la tecnología permite que la información personal sobre la salud sea hoy fácil de almacenar, actualizar, acceder e intercambiar; entre los derechos inalienables de las personas que se incluyen en esta Declaración que recoge Bollier y Firestone (2010) están:

• Tener derecho a nuestros propios datos de salud.

• Tener derecho a conocer la fuente de cada elemento de datos de salud.

• Tener derecho a acceder a una copia completa de nuestros datos de salud individuales, sin demora, a un coste mínimo o sin coste alguno; si los datos existen en forma electrónica, deben estar disponibles en esa forma.

• El derecho a compartir nuestros datos de salud con otras personas de la forma que creamos más conveniente.

El **Ordenamiento jurídico español establece** en la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal, en su título X (referido a delitos contra la intimidad, el derecho a la propia imagen y inviolabilidad del domicilio), capítulo primero (del descubrimiento y revelación de secretos), artículo 197[86], en su apartado 5 estipula que "*cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior*".

2.1.4. Historia clínica electrónica.

Aunque todavía no es un asunto prioritario en muchos jurisdicciones, la seguridad de los datos y la privacidad de los datos personales de salud son fuente de creciente preocupación general; Los EHRs transmitidos a través de redes nacionales e internacionales ofrecen oportunidades únicas para un mejor cuidado del paciente, facilitando el intercambio de datos entre profesionales, pero sólo con conexiones seguras se puede evitar un acceso o uso no autorizado. 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, define en su artículo 3 la historia clínica como "*el conjunto de documentos que*

[86] Merece la pena mencionar aquí los apartados 1 y 2:

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de de un paciente a lo largo del proceso asistencial", al mismo tiempo que define la información clínica como *"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"*.

El Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, se refiere de forma concisa y precisa al soporte de la historia clínica, señalando que:

"1.- La historia clínica se podrá elaborar en cualquier soporte documental, preferentemente electrónico, siempre que quede garantizada la autenticidad, integridad, seguridad y conservación del contenido, y su plena reproducción futura. La presentación y diseño de los datos contenidos en estos soportes ha de garantizar la continuidad de la asistencia prestada a la persona paciente, así como la factibilidad de que la historia clínica pueda ser compartida entre los y las profesionales, y los diversos centros y niveles asistenciales implicados en la atención del paciente.

2.- La historia clínica electrónica se constituye como el soporte más adecuado para la asistencia sanitaria, facilitando el manejo y accesibilidad de la documentación clínica del o de la paciente o persona usuaria, y a cuyo objeto los y las profesionales que intervienen en ella tienen el derecho de acceso y el deber de acceder y cumplimentar la historia clínica electrónica".

Hasta hace poco el personal sanitario escribía notas sobre la salud de un paciente su informe, luego esas notas se añadían a un expediente médico del paciente, que posteriormente era ampliaba según las necesidades, y además se almacenaba físicamente en el consultorio. Hoy hemos pasado a la era digital, a almacenar de una nueva manera la historia clínica de un paciente, aunque la historia clínica es un concepto que continúa en proceso de estructuración desde el punto de vista jurídico (Martínez, 2016).

La gestión de la HCE ofrece una valiosa fuente de información para la realización de estudios epidemiológicos. Todo ello implica unos desafíos técnicos y legales. Los posibles beneficios que ofrecen los sistemas de HCEs para facilitar y agilizar la atención sanitaria con menores costes a largo plazo son significativos, pero no pueden lograrse a costa de la protección de datos de carácter personal de los pacientes. La puesta en marcha de un sistema paneuropeo de salud y del acceso a datos de salud ofrecen múltiples desafíos, pero la HCE parece que acabará por imponerse en Europa, tanto en el ámbito de la sanidad pública como privada.

Sanz (2016) señala que "la privacidad, el derecho a la confidencialidad y el modo de conservar la información han sido cuestiones importantes en la implementación de la tecnología de la información en

medicina. De ahí la presencia constante de estos aspectos en el desarrollo de la historia clínica electrónica y de cualquier aplicación informática relacionada con el cuidado de la salud"[87].

La implementación y evaluación de los sistemas de información sanitaria (HIS) está plagada de problemas, las deficiencias e ineficiencias en la implementación son abundantes; Sligo, Gauld, Roberts y Villa (2017) abordan esta problemática desde distintos puntos de vista, pues su implementación es compleja y depende de factores organizativos, estructurales, tecnológicos y humanos para tener éxito. Requiere una evaluación reflexiva, matizada y multidimensional para proporcionar retroalimentación continua que asegure el éxito.

La información que se registra actualmente en la HCE puede ser mejorable, se podría ampliar, siempre que los individuos europeos perciban que su privacidad está garantizada. En una primera fase de esta investigación se ha confirmado que la vulnerabilidad reside en los jóvenes entre 15 y 24 años que hoy parecen dispuestos a renunciar a su privacidad bien a cambio de determinados servicios[88]. El análisis por edad y país de procedencia de los individuos contribuye a valorar la magnitud de los riesgos y las barreras a la armonización en la UE. Los ciudadanos españoles aparecen entre los europeos más dispuestos a facilitar su historial clínico en Internet.

Auffray et al. (2016) abordan la importancia de los registros de pacientes; estos registros han servido durante décadas como una herramienta clave para la evaluación de los resultados clínicos y del éxito de la tecnología sanitaria y de la salud. La Organización Europea para la Investigación y Tratamiento del Cáncer (EORTC) abrió un registro prospectivo de pacientes con melanoma en junio el año 2015. La Red Europea de Registros de Cáncer (ENCR), creada en el marco del Programa Europa contra el Cáncer de la Comisión Europea, promueve la colaboración entre los registros de cáncer, define las normas de recopilación de datos, proporciona formación para el personal que trata con el registro de datos de cáncer, y difunde con regularidad información sobre la incidencia y mortalidad por cáncer en la Unión Europea y otros países europeos.

Los registros de los pacientes tienen un importante potencial para la mejora de la investigación y de la salud pública en la UE, debido al gran volumen de pacientes contenidos en cada registro y la variedad de la información médica de calidad en relación con cada paciente, insisten Auffray et al. (2016); los registros de pacientes son cada vez más importantes para controlar los tratamientos de los pacientes y para la evaluación de la seguridad y la identificación de las tendencias de la medicina traslacional[89] (por ejemplo,

[87] León Sanz, 2008.

[88] Comisión Europea, Eurobarómetro especial 359 (2011).

[89] Existen diferentes concepciones de lo que significa medicina traslacional, para la Academia Europea de Pacientes (EUPATI) es "la disciplina que está avanzando rápidamente en la investigación biomédica y que pretende acelerar el descubrimiento de nuevas herramientas diagnósticas y nuevos tratamientos usando un enfoque multidisciplinar altamente colaborativo". Con frecuencia se describe como la práctica de transferir conocimiento

ensayos clínicos basados en información registral, o la medicina personalizada). Los registros de pacientes facilitan la toma de decisiones informadas de políticas a nivel nacional local, regional, e incluso a nivel internacional; como resultado, se han establecido cientos de registros desde la esfera nacional a proyectos internacionales de enfermedades raras, con utilización combinada de datos clínicos y genéticos juntos con los biobancos. No obstante, la combinación de estas fuentes de información dispares, que guían la investigación en materia de salud y la toma de decisiones clínicas, **se ha quedado atrás, por razones como la protección de datos de carácter personal y la fragmentación de los marcos regulatorios**, en el uso a gran escala y en la recogida de Big Data característica de otros sectores; ámbitos como la ingeniería electrónica y la ingeniería mecánica, y campos como la industria aeronaútica[90], la meteorología, o la robótica, han demostrado las ventajas del intercambio de datos y su experiencia podría ayudar a eliminar barreras de la investigación en el campo de la salud.

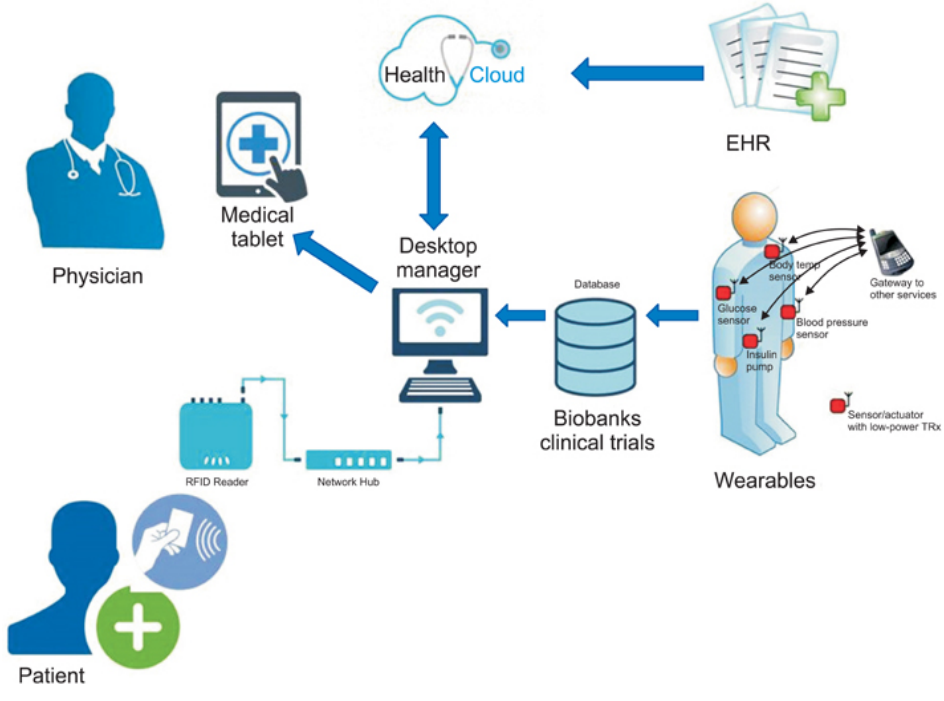
Los registros de salud electrónicos (EHR) y el uso de sistemas informáticos inteligentes están teniendo un impacto creciente respecto a enfoques tradicionales en la medicina como afirman Schoenhagen y Mehta (2016), donde el EHR más básico recoge y almacena todos los datos generados en un sistema sanitario (como por ejemplo notas médicas, resultados de pruebas y estudios de imágenes), pero donde, al margen de estos datos tradicionalmente generados dentro del entorno clínico, existen otras fuentes más novedosas de información que pueden afectar o influir en la atención sanitaria al paciente; Schoenhagen y Mehta se refieren más en concreto a los dispositivos portátiles, a la información recogida por sensores, y a las aplicaciones que capturan y rastrean diversos datos de carácter personal del entorno, datos socioeconómicos y otros datos personales que pueden ser útiles y valicosos a la hora de conocer o evaluar el estado de salud de un individuo.

En la figura 2.2. se puede ver una ilustración de cómo la revolución en *eHealth* va a transformar la relación médico-paciente de forma insólita, en el entorno del *Internet of Things;* como indica en detalle Dimitrov (2016) en esta figura, un paciente con diabetes tendrá una tarjeta de identificación, que una vez escaneada, conecta con la nube de forma segura, donde se almacenan su datos de salud electrónicos y resultados de pruebas, historial médico y prescripciones, a la vez que médicos y enfermeras acceden fácilmente a los datos desde una tableta o un ordenador.

científico desde el laboratorio a la cama del paciente, pues se basa en avances básicos de la investigación (por ejemplo, estudios de procesos biológicos que utilizan cultivos de células o modelos de animales) y a partir de ellos desarrolla nuevos tratamientos o procedimientos médicos.

[90] Kaplan et al. (2013) abordan en detalle la ingeniería de sistemas aplicada al campo de la salud en su artículo *"Bringing a systems approach to health"*.

Figura 2.2.
Hospital en el entorno de *Internet of Things* (IoT)



Fuente: Dimitrov, 2016.

Aunque parezca algo elemental, Dimitrov insiste que la adopción Electronic Health Records (EHRs) representa una verdadera revolución, un cambio en la forma tradicional de operar, en menos de 10 años se digitalizarán los datos y se reemplazará el sistema de papel y tinta, de gestión de registros que se remonta a miles de años (Kruse, Kothman, Anerobi y Abanaka, 2016). Las ventajas del nuevo escenario son numerosas y obvias; los expedientes de papel, escritos a menudo en caligrafía cuestionable, guardados en archivadores, fuera del alcance de investigadores y de otros profesionales de la atención sanitaria, dan lugar a un nuevo sistema que mantiene toda la información importante en un lugar donde puede compartirse fácilmente. Los EHRs supondrán una verdadera revolución pues evitarán muchas ineficiencias y podrán llegar a salvar vidas.

Existen desafíos técnicos que acompañan la gestión de registros electrónicos de salud, por ello Auffray et al. estiman que la adopción del EHR en toda Europa es muy variable, donde países como Estonia o regiones como la Comunidad Valenciana (España), por ejemplo, se han lanzado por completo al uso de la HCE. Mandl y Kohane (2016) hablan de los pasos que ha dado EE.UU. hacia una economía dirigida por los pacientes, donde el paciente es dueño de sus datos; este contexto requiere el desarrollo de una infraestructura adecuada de registros de salud, pero proporciona una amplia gama de nuevas oportunidades de negocio con gran potencial en servicios de salud. Capacitar a los pacientes para que tomen el control de sus datos podría ser de particular importancia para la investigación de la salud y la sanidad transfronteriza en Europa, donde la atención sanitaria está fragmentada, transferir datos médicos de un país a otro en la UE es difícil; la asunción del concepto de propiedad de sus datos por parte de los pacientes podría ayudar a superar los

obstáculos y crear nuevas formulas para estimular una economía competitiva impulsada por la salud. Por otra parte, los registros de pacientes pueden ser computacionalmente opacos, por ejemplo, en forma de texto libre, discurso grabado, o imágenes médicas; la traducción a un formato compatible con el análisis computacional se hace necesaria. Datos en diferentes idiomas, tiempo de búsqueda e identificación son otras barreras importantes. Conviene aquí mencionar las mejores prácticas para la gestión de los EHRs. El Consorcio Internacional de Investigación de Enfermedades Raras (IRDiRC) desarrolla y pone en práctica los estándares y una metodología armonizada en el marco de enfermedades y casos médicos. Distintos proyectos de colaboración europeos, como el proyecto *p-medicine* financiado por la UE[91], han creado soluciones tecnológicas integradas e innovadoras que hagan posible la investigación traslacional y el desarrollo de la **medicina personalizada, una necesidad urgente en la socidad actual**.

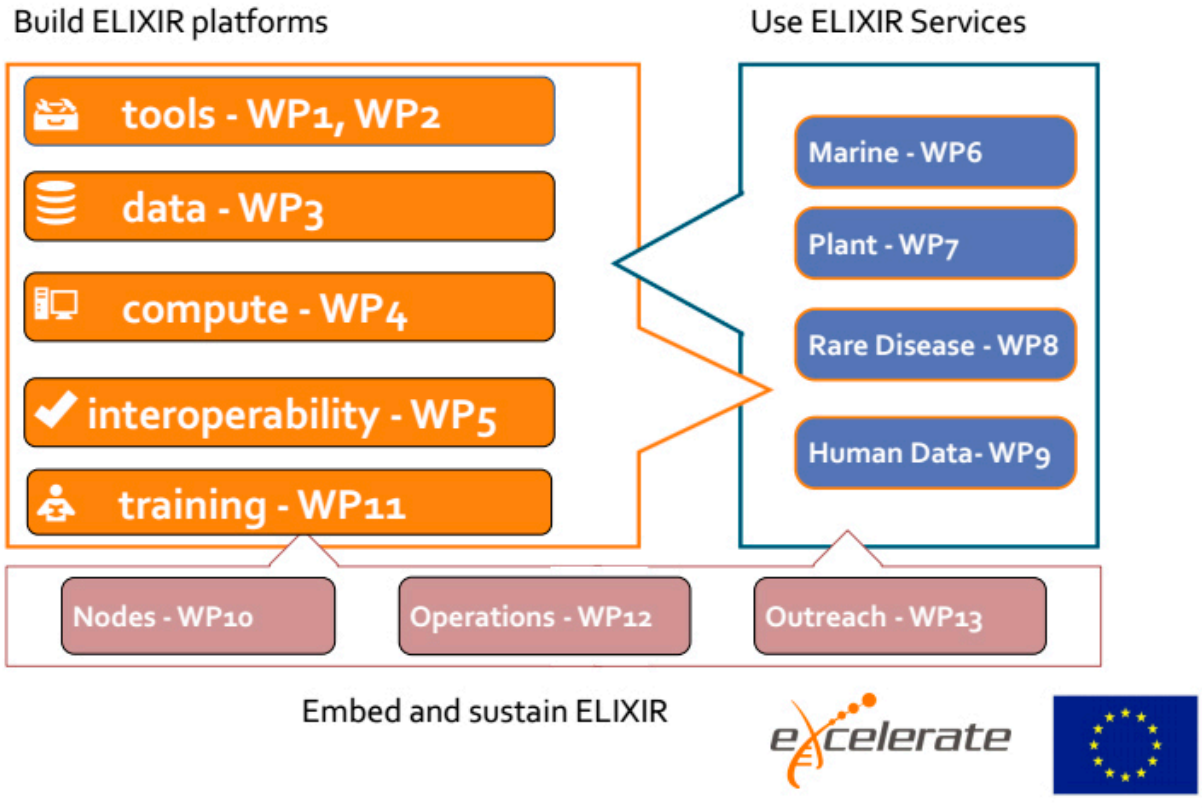
Hay que citar en este contexto proyectos como Elixir[92], la infraestructura europea para la investigación biológica, que reúne a las principales organizaciones europeas de ciencias de la vida para gestionar y salvaguardar el creciente volúmen de datos generados por la investigación; sus actividades (figura 2.3.) giran entorno a cinco áreas (datos, herramientas, cómputo, interoperabilidad y formación) y ha facilitado la recogida, el control de calidad, y el archivo de grandes cantidades de datos de ciencias de la vida, tales como datos de medicina traslacional[93], con herramientas para la presentación segura de datos.

[91] Personalized medicine. Recuperado de http://www.p-medicine.eu. Último acceso 15 noviembre de 2016.

[92] Elixir. Recuperado de https://www.elixir-europe.org. Último acceso 10 octubre de 2016.

[93] Ison et al., 2015.

Figura 2.3.
Estructura de Excelerate[94] en la infraestructura de Elixir.



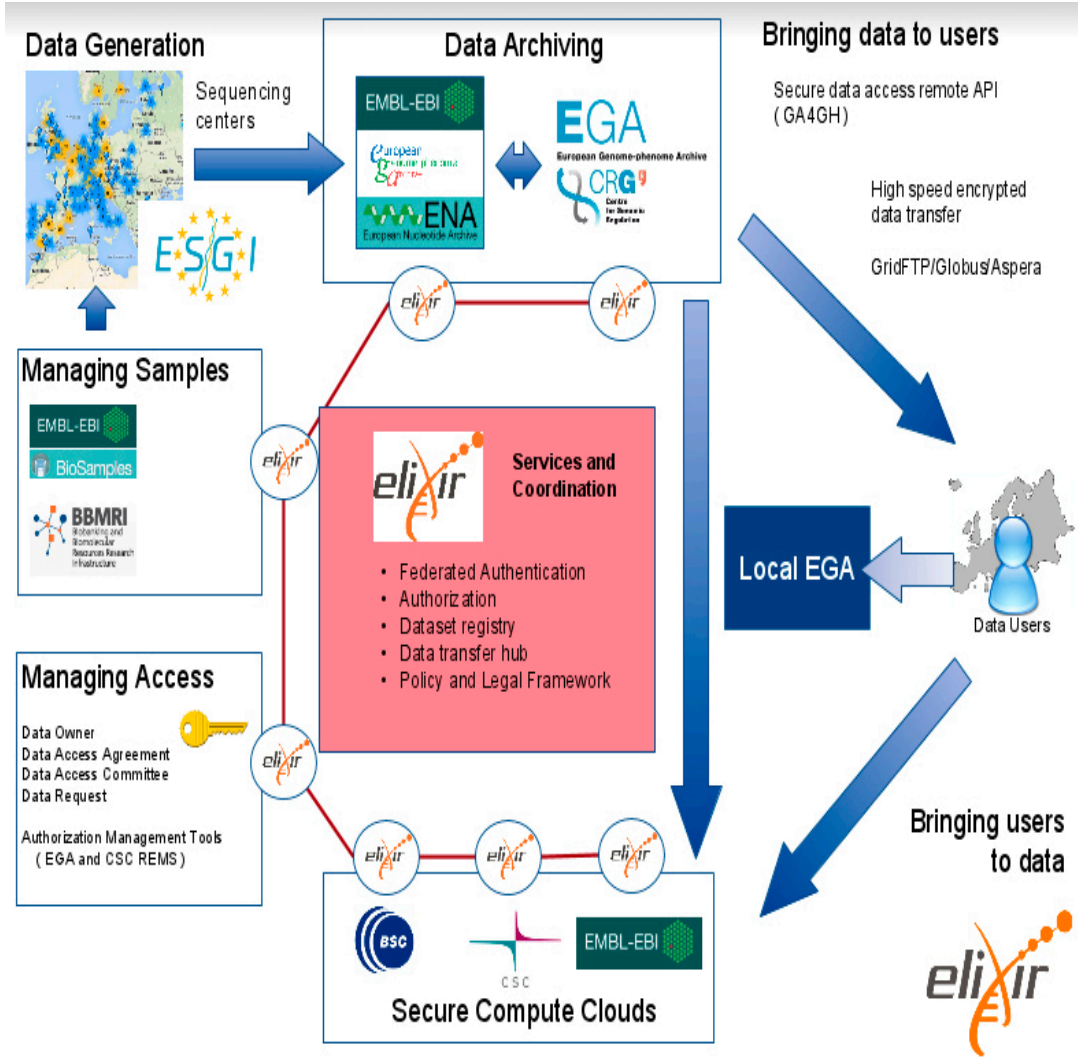
Fuente: infraestructura Elixir (www.elixir-europe.org).

En la siguiente figura 2.4. se muestra el caso de uso de datos humanos, denominado *work package 9* (WP9), en el marco de Elixir. Este caso reúne el Archivo Genómico-Fenómeno Europeo (EGA[95]) y otros socios para proporcionar una plataforma Elixir para datos biomédicos humanos con control de acceso. Este caso proporciona un flujo de trabajo para el almacenamiento a largo plazo y la reutilización de datos biomédicos humanos. Este flujo de trabajo y la infraestructura de soporte permiten a los titulares de los datos concentrarse en sus áreas de generación de datos y experiencia en análisis, mientras puedan confiar en EGA y la infraestructura de Elixir para sus necesidades comunes de almacenamiento, coordinación y distribución de datos dentro de marcos legales correspondientes.

[94] Excelerate es un proyecto que forma parte de Elixir y pretende implementar su infraestructura y desarrollar sus plataformas; se trata de la coordinación y ampliación de recursos de datos nacionales e internacionales para asegurar la prestación de servicios de datos de ciencias de la vida de primer nivel, apoyando un programa de formación paneuropeo, anclado en las infraestructuras nacionales, para aumentar la capacidad y la competencia bioinformática. También proporciona eficiencias en la gestión y operación en toda la infraestructura, en un entorno geográfico que incluye 17 países (Excelerate. Recuperado de https://www.elixir-europe.org/excelerate. Último acceso 16 octubre de 2016).

[95] European Genome-phenome Archive

Figura 2.4.
WP9 - Marco de trabajo de Elixir para el archivo, la diseminación y el análisis seguro de datos humanos con control de acceso



Fuente: infraestructura Elixir (proyecto Elixir)

Por otro lado, se ha investigado el proceso de adopción del EHR, identificando barreras y facilitadores; así, Kruse, Kothman, Anerobi y Abanaka (2016) han constatado que la mayoría de los facilitadores son la eficiencia, el tamaño del hospital, la calidad, el acceso a los datos, el valor percibido y la capacidad de transferir información, a la vez que señalan barreras para la adopción del EHR como el coste, inversión en tiempo, la percepción de inutilidad, transición de datos, la localización de instalaciones y problemas de implementación.

En conclusión, como afirma Zhang (2014) los médicos y los investigadores del ámbito médico y científico deben hacer todo lo que esté a su disposición para el uso del Big Data que continuamente se genera en un sistema de EMR (*electronic medical record*) y otras bases de datos de salud; Zhang entiende que supone una perdida de recursos el hecho de dejar los datos electrónicos registrados sin más en un disco,

sin explorar su valor potencial para revelar los mecanismos que subyacen al desarrollo de una enfermedad, algo que reivindica en el mayor mercado del mundo, China, con toda su capacidad para contribuir a la investigación médica. Estoy de acuerdo con esta afirmación si bien es cierto que no parece muy preocupado por los derechos individuales, cuando no se pueden olvidar los límites que deben existir siempre desde el punto de vista de la privacidad, con mayor peso y razones en entornos de regímenes sin una base democrática. Zhang (2015) destaca en un artículo posterior (titulado "*Data management by using R: big data clinical research series"*), que frente al sistema tradicional de registro por escrito, el EMR hace que la investigación médica con Big Data sea viable; la característica más importante de la investigación del Big Data es su configuración en el mundo real, además la investigación del Big Data puede proporcionar todos los aspectos de la información relacionada con la asistencia sanitaria. Pero **la investigación con Big Data requiere algunas habilidades en la gestión de los datos**, que sin embargo brillan por su ausencia en la formación de muchos médicos, lo que dificulta en gran medida que los médicos puedan probar su hipótesis clínica mediante el uso de EMR.

2.2. El derecho fundamental a la protección de datos.

La Constitución Europea has reconocido el derecho fundamental a la protección de datos. Asimismo determina que todos los países miembros de la UE deberán contar con una autoridad independiente que debe garantizar y tutelar este derecho. En España es la Agencia Española de Protección de Datos (AEPD) la encargada de tutelar y garantizar el derecho. Se trata de un derecho que nace en Europa y que está en proceso de expansión global.

2.2.1 Introducción.

Como bien apunta Greenleaf (2015) cada día es mayor el número de países que promulgan leyes de protección de datos, con 111 países que han seguido la estela del modelo europeo y la influencia del Convenio 108 del Consejo de Europa (Greenleaf, 2016); tal y cómo ha documentado ya en 2011 eran 76 países (Greenleaf, 2011), pasando a ser 89 a principios de 2012 (Greenleaf, 2012), y 99 en 2013 (Greenleaf, 2013), para llegar a 109 en 2015. Parece una tendencia creciente a nivel internacional que se vayan implementando legislaciones en esta dirección, aunque regiones como Asia están muy atrás en el desarrollo de leyes de privacidad si lo comparamos con otras regiones del mundo, especialmente Europa y América (Li, 2015). Aún así se están aprobando leyes de protección de datos incluso en países como Kazajistán (siguiendo la estela de Kirguistán, primer país en Asia Central en aprobar una ley de datos de carácter personal en 2008); se trata de la jurisdicción no. 100 del mundo en promulgar una ley de protección de datos,

un estado autoritario con régimen de partido único (su presidente Nursultan Nazarbayev lleva en el poder desde 1990), y sin antecedentes de respeto de las libertades civiles, pero a pesar de sus limitaciones y posibilidades de cuestionable aplicación, la ley (promulgada el 21 de mayo de 2013 y que entró en vigor el 26 de noviembre de 2013) abarca aspectos a los que cualquiera de las empresas que hacen negocios en o con Kazajistán deben dar seria consideración, sobre todo debido a la posibilidad de enfoques muy divergentes entre las diferentes agencias gubernamentales (Greenleaf, 2013); la legislación de Kazajistán ilustra como pocas la **diferencia entre promulgar una ley de protección de datos y garantizar una protección efectiva, algo vinculado al estado de las libertades civiles**. En todo caso, el que resulta ser mayor movimiento plurijurisdicccional a nivel global hasta la fecha, en esta materia, ha sido la celebración de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos en la Cumbre de la Unión Africana en Malabo, Guinea Ecuatorial (27 de junio de 2014), con 54 Estados miembros, aunque su relevancia futura dependerá de las adhesiones y ratificaciones según Greenleaf y Georges (2014).

2.2.2. El derecho fundamental en Europa.

El Consejo de Europa tiene su origen justo después de la Segunda Guerra Mundial para reunir a los Estados de Europa para promover el Estado de Derecho, los derechos humanos, el desarrollo social y la democracia. El Convenio Europeo de Derechos Humanos (ECHR[96]) se aprobó con este fin en 1950[97], incluyendo el germen del derecho a la protección de datos personales, en su artículo 8 (derecho al respeto a la vida privada y familiar), que determina:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Pero para poder entender en toda su extensión el derecho fundamental a la protección de datos de carácter personal es preciso atender al Convenio 108 del Consejo de Europa (1981) y a los instrumentos de la UE como las Directivas, que tanto han contribuido a la armonización de la protección de datos en Europa, junto con la jurisprudencia del TJUE y el Tribunal Europeo de Derechos Humanos.

[96] Acrónimo del inglés "*European Convention of Human Rights*".

[97] Aunque entró en vigor en 1953.

Los tratados fundacionales de las Comunidades Europeas no contienen ninguna referencia a los derechos humanos ni a su protección. Sin embargo, se presentaron demandas ante el entonces llamado Tribunal Europeo de Justicia (ECJ[98]), alegando violaciones de derechos humanos en áreas dentro del ámbito del derecho europeo, lo que motivó el desarrollo de un nuevo enfoque[99]; con el fin de otorgar protección a los particulares, se incorporaron derechos fundamentales a los llamados principios generales del derecho europeo. Así, el TJUE[100] confirmó que garantizaría el cumplimiento de estos principios. En el año 2000 la UE proclamó la Carta de los Derechos Fundamentales de la Unión Europea, cuyo artículo 8 recoge la protección de datos personales; aunque en un principio sólo se trataba de un documento político, con la entrada en vigor el 1 de diciembre de 2009 del Tratado de Lisboa (firmado el 13 de diciembre de 2007), la Carta de Derechos Fundamentales de la UE se hizo jurídicamente vinculante, con lo que el derecho a la protección de datos personales pasó a ser un derecho fundamental independiente. El Reglamento (EU) 168/2007 del Consejo, de 15 de febrero de 2007, creó una Agencia de los Derechos Fundamentales (FRA), que proporciona a las instituciones y gobiernos de la UE ayuda en lo que se refiere a derechos fundamentales a la hora de aplicar el Derecho de la UE; se crea así un organismo específico para los derechos fundamentales a nivel de la UE y se detallan sus principales cometidos y objetivos, el funcionamiento y la gestión interna. La Agencia pone medios para la protección de datos incluidos manuales para profesionales de la justicia; estos manuales incluyen y presentan la jurisprudencia y la legislación de la UE de modo accesible. Esta Agencia ha abordado temas como asilo, fronteras e inmigración, no discriminación y también protección de datos.

El Tratado de Funcionamiento de la Unión Europea en su artículo 16 y el Tratado de la Unión Europea en su artículo 39 abordan expresamente este derecho. Pero son las Directivas las que han lo conformado e influido directamente en las legislaciones de cada Estado miembro:

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

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

[98] European Court of Justice.

[99] Consejo de Europa y FRA. Handbook on European Data Protection Law. Recuperado de http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf. Último acceso 13 enero 2017.

[100] La función del TJUE es "garantizar que la legislación de la UE se interprete y aplique de la misma manera en cada uno de los países miembros; garantizar que los países miembros y las instituciones europeas cumplan la legislación de la UE" de acuerdo con https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_es. Último acceso 2 enero de 2017.

-Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

La Directiva 95/46/CE ha consagrado dos de las ambiciones más antiguas e igualmente importantes del **proceso de integración europea**, a saber, la protección de los derechos y libertades fundamentales de las personas y, en particular, el derecho fundamental a la protección de datos, por una parte, y la realización del mercado interior (con la libre circulación de los datos personales).

El 25 enero 2012 la Comisión Europea propuso la reforma profunda de las normas de protección de datos en la UE, para el establecimiento de normas de protección de datos en la era digital **poniendo a los ciudadanos en control sobre sus propios datos personales**, a la vez que se quería simplificar el entorno regulador para las empresas que operan en la UE (reducir los costes). El resultado es el nuevo RGPD (ver apartado 4.6.), clave para el proyecto del mercado único digital, con el objetivo de capacitar a los ciudadanos y empresas europeos para que se puedan aprovechar todas las oportunidades que ofrece la economía digital[101], también en el área de la salud.

2.2.3. La protección de datos en España.

En España regulado en el artículo 18.4 de la Constitución Española (1978), que debe diferenciarse del derecho a la intimidad del artículo 18.1 CE (con el que guarda la similitud de ofrecer una especial protección constitucional -la vida privada, personal y familiar-), atribuye a su titular un conjunto de facultades que esencialmente imponen a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley. Como bien determina la STC 292/2000, el derecho que se somete a exámen atribuye a su titular la facultad de "controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención". La jurisprudencia ha consolidado en España "**la consideración de la protección de datos como un derecho autónomo e independiente**"[102]; así esta sentencia, en su fundamento jurídico séptimo recoge:

*"7... el contenido del Derecho fundamental a la protección de datos consiste 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*

[101] Comisión Europea. Data Protection Eurobarometer Factsheet. Recuperado de: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf. Último acceso 12 diciembre 2016.

[102] Mañas (2009).

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 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. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

Pues bien, el artículo 2.a) de 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, señala que **los datos personales son "toda información sobre una persona física identificada o identificable", especificando que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".** Que los datos permitan o no identificar a la persona es fundamental, porque si (la recogida, procesamiento o uso de datos) no lo permiten, el derecho del individuo a la intimidad no se verá amenazado, al menos en el mismo grado (Dwork y Mulligan, 2013; Lloyd, 2014; Tene, 2007).

Anterior a este Directiva de 1995, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), estuvo vigente hasta el 14 de enero de 2000, cuando entró en vigor la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que más tarde se acompañó del Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD). Adicionalmente en España hay que atender a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, asi como a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Como indica Mañas (2009) “pasa así a un segundo plano la discusión acerca de qué se entiende por privacidad o intimidad”, porque el núcleo protector del derecho a la protección de datos se extiende a todo tipo de datos, de cualquier naturaleza, independientemente de que unos, “por su especial naturaleza, requieran de mayor protección que otros. Este sería el caso de los llamados datos sensibles o especialmente protegidos (a los que se refiere el artículo 7 de la LOPD)”.

2.3. La Protección de los datos de salud.

Hay que atender a la Directiva de protección de datos 95/46/CE y a la Directiva sobre la privacidad y comunicaciones electrónicas 2002/58/CE. En España la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal transpone la Directiva 95/46/CE. Por otro lado la AEPD ha emitido una serie de informes jurídicos que detallan cómo debe interpretarse la Ley en relación con los datos da salud[103].

La datos relacionados con la salud de los individuos reciben una protección especial en Europa, que no es arbitraria como recuerda la AEPD[104], pues es consecuencia de lo que se dispone en las normas Comunitarias que regulan el tratamiento automatizado de datos de carácter personal. En este sentido, el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, y el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (aprobado en Estrasburgo el 28 de enero de 1981, y ratificado por España en fecha 27 de enero de 1984), hacen referencia específica a los datos de salud como sujetos a un régimen especial de protección; dicho Convenio determina que los datos de salud "no podrán tratarse automáticamente a menos que el derecho interno prevea garantías adecuadas".

El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, como recuerda la AEPD, ya viene a definir la noción de "datos de carácter personal relativos a la salud", considerando que su concepto abarca **"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo"**, y puede referirse a informaciones sobre un individuo de buena salud, enfermo o fallecido, y que además "debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas"[105]; en este mismo sentido, la Recomendación no R (97) 5, del Comité de Ministros del Consejo de Europa, relativa a la protección de datos médicos establece que "la

[103] Informes Jurídicos 1999/2000, 2000/0000, 2002/0359, 2003/0381, 2003/0526, 2004/0036, 2004/0182, 2004/0409, 2004/0449, 2005/0025, 2005/0042, 2005/0129, 2005/0164, 2005/0248, 2005/0304, 2005/0369, 2006/0005, 2006/0012, 2006/0018, 2006/0114, 2007/0496, 2008/0471, 2008/0488, 2008/0617, 2008/0656, 2009/0525, 2011/0262, 2011/0268, 2014/0222.

[104] AEPD. Informe Jurídico 2008/0488.

[105] AEPD. Informe Jurídico 1999/0000.

expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas". Se debe entender que los datos psicológicos, psiquiátricos y referentes a la salud mental[106] de las personas también quedan incluidos en este concepto y reciben especial protección de la Ley, de acuerdo a la AEPD baste recordar la existencia de la Recomendación no R (91) 15 del Comité de Ministros, en materia de estudios epidemiológicos en el ámbito de la salud mental, en donde se hace expresa mención a la necesidad de fijar las garantías necesarias para la protección de los datos en caso de trastornos. Estos datos de salud, aún cuando no provengan expresamente del historial clínico de los pacientes, confirma la AEPD que deben ser considerados como datos relativos a la salud de las personas; es el caso del ADN, pues aunque se un análisis de ADN no codificante no se deriven directamente datos de salud, los resultados constituyen la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con su salud[107].

El artículo 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (que transpone en España la Directiva 95/46/CE), estipula: *"**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**"*, a pesar de ello el artículo 11.2 f) de esta Ley especifíca que *"el consentimiento exigido en el apartado anterior no será preciso...cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica"*.

La regla general para **la recogida y el tratamiento de los datos de salud consiste en exigir el consentimiento libre, inequívoco, informado y expreso de los afectados**, sin perjuicio de lo señalado en la normativa estatal y autonómica respectivamente en cuanto a las historias clínicas.[108]

La comunicación de datos de enfermedades, solicitada por organismos públicos con identificación de personas (datos de carácter personal incluidos nombre, apellidos, DNI, fecha de nacimiento, domicilio, etc.), para ser incorporados a un registro[109] debe ser considerada una transmisión de datos que constituye una cesión de datos de carácter personal, que queda definida por el artículo 3 i) de la Ley Orgánica 15/1999, de

[106] Flores (2010) afirma que Europa es es la región del mundo con la más abundante normativa sobre salud mental, especialmente en forma de recomendaciones dirigidas a los Estados por el Consejo de Europa, no obstante recuerda que también existen normas de aplicación directa: Convenio Europeo de Derechos y Libertades Fundamentales y Convenio de Biomedicina.

[107] AEPD. Informe Jurídico 2000/0000.

[108] AEPD. Informe Jurídico 2008/0471.

[109] AEPD. Informe Jurídico 2011/0262.

13 de diciembre, de Protección de datos de Carácter Personal, como "toda revelación de datos realizada a una persona distinta del interesado".

Siempre habrá que poner estos principios en contexto, por lo que habrá que atender a lo que otras leyes sectoriales puedan determinar, en este caso la Ley 14/1986, de 25 de abril, General de Sanidad, que estipula en su artículo 8.1 lo siguiente: *"Se considera como actividad fundamental del sistema sanitario la realización de los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiólogica". Por otro lado, en relación con la salud individual y colectiva que se regula en el capítulo V de la misma Ley 14/1986, su artículo 23 establece que "Para la consecución de los objetivos que se desarrollan en el presente Capítulo, las Administraciones sanitarias, de acuerdo con sus competencias, crearán los registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria".*

En lo referido a la organización de los sistemas de información (bases de datos) hay que atender a lo que establece la Ley 33/2011, de 4 de octubre, General de Salud Pública, que en su artículo 41 estipula:

*"1. Las **autoridades sanitarias** con el fin de asegurar la mejor tutela de la salud de la población podrán requerir, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria.*

*2. Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello **sea estrictamente necesario para la tutela de la salud de la población**.*

3. A los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública se someterá a lo dispuesto en el apartado 3 del artículo 16 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."

Este artículo 16.3 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, regula el acceso a la historia clínica determinando la forma y fines del mismo, y 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

*de Carácter Personal, 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 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, 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."

La AEPD establece, si bien con carácter general el acceso a datos contenidos en las historias clínicas con fines epidemiológicos debe llevarse a cabo de forma que **queden disociados los datos de carácter personal de los de carácter clínico-asistencial**, la propia norma recoge la posibilidad de que las Administraciones sanitarias accedan, en los términos señalados en el precepto transcrito, a los datos identificativos de los pacientes por razones epidemiológicas cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población.

Muchos registros actualmente (como los relacionados con el cáncer, por ejemplo, con su magnitud como enfermedad, su evolución, la distribución espacial de la incidencia y la supervivencia, o la evaluación clínica) "no están suficientemente dotados, generando retrasos y mermando posibilidades de explotación de la información" como indicaba la Estrategia en Cáncer, aprobada el 29 de marzo de 2006, en el Consejo Interterritorial del Sistema Nacional de Salud (España)[110], al señalar que "los registros poblacionales de cáncer existentes en el momento actual, que permiten conocer aspectos esenciales de este problema de salud—además, que su cobertura territorial es parcial, no pudiendo conocerse todos estos aspectos en diversas zonas geográficas. Dicha razones justificaban que dicha Estrategia incluyese entre sus objetivos el de promover la mejora y extensión de los registros poblacionales de cáncer, de forma que permitiesen cubrir, con suficiente calidad y representatividad, aquellos aspectos y territorios deficitarios".

La AEPD es clara en este sentido, en lo que a los registros de enfermedades como el cáncer se refiere, la necesidad de conocer datos referidos a la supervivencia o a la evaluación clínica exige el conocimiento y la incorporación a los registros de datos identificativos de los pacientes. Se trata por lo tanto

[110] AEPD. Informe Jurídico 2011/0262.

para la AEPD de un supuesto incluido en el último párrafo del artículo 16.3 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 **ampara la comunicación de datos sin necesidad de consentimiento del titular del dato**. En cualquier caso, la AEPD señala que siempre se deben respetar siempre los principios de protección de datos que se recogen en el artículo 4 de la Ley Orgánica 15/1999, en su apartado 1: "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean **adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas** para las que se hayan obtenido", a la vez que la AEPD recuerda en aquellos casos en que no se hace necesario el consentimiento del interesado para una cesión de datos de carácter personal, queda siempre obligado el responsable del fichero a informar al interesado sobre los destinatarios de la información, en el preciso momento en que se recaben los datos[111].

2.4. Internet y la salud.

La llegada de las nuevas tecnologías obliga a analizar la repercusión de Internet en el derecho fundamental a la protección de datos de carácter personal, pues "la sensación de libertad que el potencial consumidor o usuario experimenta en materia de comercio electrónico únicamente puede calificarse de falaz pues es simple apariencia" (López Jiménez, 2009). Interconectar diversos dispositivos supone someternos a riesgos y amenzas, especialmente en tiempos de IoT (Hu, 2016). Según de desprende de la encuesta de la Comisión Europea "*Flash Eurobarometer 404*" (2014) un 59% de los ciudadanos europeos utilizan Internet como fuente de información sobre salud[112] (en el apartado 3.3. se abordan en detalle las actitudes de los ciudadanos europeos respecto a la salud, la protección de datos e Internet).

2.4.1. Internet y las redes sociales.

Según el principio de la inteligencia colectiva, Lévy (2004) señala que una red parte de dos principios básicos, siendo uno de ellos el hecho de que los seres humanos vivimos en sociedad (interactuamos unos con otros lo que representa un sistema de aprendizaje en sí mismo), y el segundo consiste en que las interacciones funcionan de forma similar a un sistema neuronal; con nuestras interacciones con las cosas vamos desarrollando competencias, es decir, a través de nuestra relación con los

[111] Artículo 5 de la Ley orgánica 15/1999.

[112] Principalmente para asuntos relativos a estilos de vida saludables y bienestar psicológico.

signos y con la información es cómo adquirimos nuevos conocimientos. Y en un momento posterior en relación con otras personas, por medio de la transmisión hacemos vivir el conocimiento. Se trata de tres maneras complementarias de la transacción cognitiva que pasan incesantemente del uno al otro: competencia, conocimiento y saber. Para Lévy cada actividad, cada relación humana, cada acto de comunicación, representa un aprendizaje; el transcurso de la vida, por las competencias y los conocimientos que abarca, alimenta un circuito de intercambio o lo que llama **sociabilidad de conocimiento.**

Castells (2001) ya hablaba de la sociabilidad en Internet, de la interacción social o individual en Internet y las comunidades virtuales de Internet, un tema decía "dominado por las fantasías de los futurólogos y de los periodistas no bien informados". Esta investigación se has inspirado en las redes sociales como fuente de datos y su utilidad como herramienta de estimación (Moreno Reyes, Puelles Gayo, y Kress, 2017) y ha tomado en cuenta ideas como la contenida en el artículo escrito por Jon Gertner "Social Media as Social Index" (2010) del "10th Annual Year in Ideas of The New York Times"; referido a las redes sociales como fuente de datos precisamente (y sus consecuencias como índice social). Se trata de una materia de enorme trascendencia, de tal forma que hasta Cameron Marlow, el responsable del equipo de analistas de datos de Facebook, afirma que parece improbable que las redes sociales no se vayan a convertir en la herramienta para realizar estudios de opinión. Gertner (2010) afirma que Internet y las redes sociales podrían ser muy útiles no sólo para realizar investigaciones de mercado, pero para todas las áreas de investigación comercial y marketing. Puesto que estas redes generan ingentes cantidades de información se pueden aplicar técnicas de análisis de datos para sacar conclusiones y poder así también estimar un comportamiento o influir en el mismo (Guidi, Ruíz-Agundez, Canga-Sánchez, 2013).

Hoy en día uno de los sectores más dinámicos del mundo en la era del Big Data son las TIC aplicadas a las *social networking sites (SNS*) o redes sociales; Internet y las redes sociales son un medio empleado cada vez con mayor frecuencia no sólo en la búsqueda de información por parte de los pacientes, sino también a la hora de compartir información; ya no sólo estamos en Internet, ahora se vive en Internet, y los pacientes son los portavoces de sus propias vivencias, en primera persona. El crecimiento de estas redes es un indicador de que hemos pasado de la era de los buscadores y webs estáticas a sistemas vivos como son las SNS. Estas SNS se enfrentan cada día a mayores retos en la protección de datos y privacidad de los usuarios, sobre todo cuando entran en juego datos especialmente protegidos, como son los datos de salud. Pero estas redes sociales también sirven para medir el *status quo* en cado momento (Gyarmati y Trinh, 2013). Por ello conviene analizar el concepto de red social, sus modalidades, y los riesgos concretos que a efectos de privacidad existen.

El tratamiento de la información debe ajustarse a prácticas lícitas y acordes con los derechos de las personas, pues son los legítimos titulares de la información; el individuo, motor de la Innovación, cobra

personalidad propia a la vez que utiliza todos los nuevos recursos a su alcance como las redes sociales y las webs especializadas que contribuyen a la explosión del Big Data. Redes como Facebook, LinkedIn y Twitter se han convertido en los sitios de Internet más populares incluso que Google. La información sensible de los usuarios no se debe compartir con terceros sin consentimiento del usuario ¿pero se protege realmente este derecho?. El seguimiento no autorizado de dichos datos constituye un hecho grave pero aún mayor trascendencia tendría el tratamiento no autorizado y la cesión de los datos. Este tratamiento representa enormes oportunidades para numerosas compañías que desean sacar beneficio de esas plataformas casi ilimitadas de información sobre sus usuarios, cuyos datos personales desean agrupar y segmentar.

A medida que las redes sociales crecen y se desarrollan, la información que los usuarios exponen en la red tiene implicaciones potencialmente peligrosas para su privacidad individual, pero como recogen Thomas, Grier y Nicol (2010) mientras que las redes sociales permiten a los usuarios restringir el acceso a sus datos personales (yo añadiría que al menos teóricamente), no existe actualmente un mecanismo que ponga en práctica o atienda las preocupaciones acerca de la privacidad sobre el contenido cargado por otros usuarios; es decir, en el caso de fotos e historias de grupo, por ejemplo, que son compartidos por nuestros amigos y familiares, la privacidad individual se escapa más allá de la discreción de lo que cada individuo colgamos en Internet, y pasa a ser un asunto más bien ajeno, dependiente de lo que cada miembro de nuestra red quiera revelar etc.

Así, un enorme volumen de información personal, incluidos los datos de salud, sobre millones de individuos, están almacenados en servidores, o en la nube, en bases de datos o incluso circulando por Internet, de una manera nunca vista antes. Las empresas, organismos y los propios usuarios de la TIC no son conscientes, en muchas ocasiones, de los riesgos para la privacidad que conlleva la inclusión de información en medios digitales o consultas sobre temas de salud en SNS (Moore, 2010). La información personal contenida en nuestras redes sociales ha sido utilizada por empleadores con fines laborales como bien apuntan Thomas, Grier y Nicol (2010), por ello hay que estar alerta no sólo al acceso a esos datos personales (relativos, por ejemplo, a enfermedades terminales o crónicas) sino al uso que se pueda hacer de los mismos, fines que pueden no estar relacionados con la investigación médica, puesto que esos mismo datos en manos de aseguradoras o empleadores podrían tener, más que beneficio para la salud y la vida del interesado, un claro perjucio para el individuo en cuestión.

Si bien es cierto, que un creciente número de comunidades digitales, redes sociales dedicadas a la salud, ofrecen a los individuos la oportunidad de recibir información, consejo, y apoyo de terceros (Centola y Van de Rijt, 2015). Esta tendencia apunta a la idea de transformación de la relación profesional sanitario-paciente, de una seria crisis del modelo tradicional (que se puede considerar paternalista), **tanto en el uso como en el acceso a la información**; se puede decir que Internet ha transformado profundamente la forma

cómo los pacientes buscan información y, en consecuencia, el diálogo tradicional entre pacientes y sus proveedores de salud (Bylund et al., 2007).

Por todo ello queda mucho por hacer ahora que se plantean muchos retos en la protección de la privacidad en el sector de *eHealth*, que afectan directamente a pacientes, profesionales, y empresas u organismos públicos y privados. Los nuevos sistemas vivos (SNS) han contribuido a crear redes globales, en las que participan activamente millones de agentes y usuarios de los servicios de *eHealth* (médicos, pacientes, farmacéuticos, etcétera). Todo ello conlleva numerosos riesgos para la privacidad pero saber afrontar dichos riesgos, identificarlos (con información y formación, pues existe todavía un enorme desconocimiento al respecto), proteger la privacidad de manera comprometida, puede representar una ventaja competitiva (Islam y Iannella, 2012).

Existen grandes riesgos para las empresas del sector *eHealth* si no gestionan correctamente los datos de sus clientes/pacientes, incluida la actuación de los profesionales. Existe una gran abundancia de datos de carácter personal referidos a la salud y el actual sistema de salud parece ineficiente. En este sentido, conviene recordar que el modelo de negocio y el funcionamiento de las redes sociales se basa tanto en la publicidad de anunciantes como en la minería de datos de los usuarios para ejecutar acciones de marketing (Aggarwal, 2011), por lo que es el marketing quién más y mejor se beneficia de los datos.

2.4.2. Internet y los buscadores.

Los motores de búsqueda son una herramientas que pone en contacto a usuarios[113] de Internet con la información de cualquier clase que se desee buscar, incluida la salud (ver apartado 3.3.); Castro (2015) señala cómo la relación de los motores de búsqueda con los datos personales se desarrolla en dos direcciones; por un lado, respecto a los datos de carácter personal del usuario que realiza búsquedas (ya que esta información permite al buscador ser más exacto y las posibilidades de explotación lucrativa de los datos personales, por parte del motor, son mayores). Y por otro, los motores de búsqueda dirigen a páginas web que pueden contener datos de carácter personal de terceros (de forma que estos datos pueden ser obtenidos fácilmente por los internautas).

[113] Cañedo Andalia (2011) defiende la necesidad de abandonar el arraigado hábito incluso entre los propios profesionales de la salud, ante un problema de información, de acudir a consultar buscadores como Google (ni siquiera Google Académico) para buscar algun dato que les permita resolverlo, y pide por ello "potenciar el uso adecuado de fuentes de información acreditadas por prominentes organizaciones y grupos científicos en materia de salud en lugar de buscadores generales como Google".

Una gran mayoría de ciudadanos europeos[114] (87%) que han buscado información general sobre salud en Internet lo han hecho para sí mismos, o tratado de obtener información sobre su propio estado de salud (78%), o han buscado una segunda opinión para su caso personal (78%), o para encontrar un tratamiento médico a su estado de salud (76%)[115]; en el apartado 3.3 aborda con mayor grado de detalle los usos y costumbres de la ciudadanos europeos en el contexto de Internet; así, existen estudios en Europa que confirman tesis como la defendida por Bylund et al. (2012) respecto al papel que desempeña Internet en el tratamiento de enfermedades en general, y en la asistencia a enfermos de cáncer en particular.

El líder indiscutible de los motores de búsqueda es Google; que compila registros de búsqueda individuales, que contienen información sobre los miedos y expectativas de los usuarios, intereses y pasiones, y que contienen información financiera, médica, sexual, política, en pocas palabras, de carácter personal (Tene, 2007); cabe por ello preguntarse ¿cómo ha evolucionado Google de ser un gigante benevolente que busca no hacer mal alguno, para convertirse en una amenaza a la privacidad que los defensores de los derechos humanos en todo el mundo denigran? ¿están justificados o son más bien exagerados los temores de la omnipresencia de Google? ¿qué datos personales debe conservar Google y por cuánto tiempo?.

La salud pública y la biomedicina constituyen una de las temáticas con mayor demanda de información en Internet; sólo en EE.UU. ya en el año 2002 cerca de 100 millones de personas navegaron por Internet en busca de información en el campo de la salud[116]. Los contenidos que se encuentran en la red son, por su volumen, accesibilidad, calidad y variedad, el recurso de información más relevante y fácil en medicina hoy día.

Con Internet nos enfrentamos al problema de determinar la ley aplicable y la jurisdicción (Gregorio, 2004). Habrá que atenerse no sólo a la legislación en vigor, sino a la jurisprudencia que modula la aplicación de la ley en última instancia. Así De Miguel Asensio (2014) se acerca al tratamiento de los datos personales por buscadores de Internet, en especial tras la sentencia sobre *Google Spain* del Tribunal de Justicia de la UE. La reciente jurisprudencia del Tribunal de Justicia aborda el ámbito de aplicación espacial de la legislación europea sobre protección de datos personales, con especial referencia al sometimiento del editor del motor de búsqueda -Google Inc.- a la legislación española de protección de datos, aspectos relativos al ámbito de aplicación espacial de la legislación europea sobre protección de datos de carácter personal, pues el domicilio social de Google Inc. se encuentra en California. El gestor del motor de búsqueda es el responsable del tratamiento, y asume obligaciones como motor de búsqueda. Resulta de especial interés

[114] Entendido como ciudadanos miembros de la UE.

[115] Datos de la Comisión Europea, encuesta "Flash Eurobarometer 404" (2014).

[116] Rodríguez Camiño, R. Motores de búsqueda sobre salud en Internet. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000500002. Último acceso 10 noviembre de 2016.

señalar que alguno de los aspectos de la resolución (que han sido objeto de importantes críticas) aparecen vinculados a la posición de claro dominio de Google en el sector de las búsquedas por Internet, tanto en España como en el conjunto de la UE. La sentencia sobre *Google Spain* resulta de especial interés en relación con las actividades a nivel nacional que desarrollan operadores cuyo establecimiento principal se encuentra fuera de la UE, aspecto de trascendencia práctica no sólo para los motores de búsqueda sino también para las redes sociales.

Según Castro (2015), siempre en relación con el caso *Google Spain*, en la medida en que afirma "se hace responsable del tratamiento al proveedor del servicio del motor de búsqueda en Internet y se predica el deber de dicho proveedor de garantizar que el tratamiento de datos que realiza cumple con los requisitos de la Directiva[117] sobre protección de datos, se produce la contraposición entre los derechos de las personas sobre las que versa la información en internet y los derechos de los usuarios del motor de búsqueda". Por un lado, de acuerdo con el artículo 12.b) de la Directiva sobre protección de datos el propio "interesado puede ejercer frente al responsable del tratamiento los derechos de rectificación, supresión y bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva", y por otro lado, de acuerdo "con el artículo 14.a) de la Directiva el interesado podrá ejercer un derecho de oposición, también frente al responsable del tratamiento"; así nos enfrentamos a derechos opuestos, los del interesado, los de los internautas en cuanto a la libertad de información, y el derecho de los proveedores de motores de búsqueda a ofrecer en el mercado productos y servicios de esta índole. Castro (2015) recuerda que estos derechos que aparecen enfrentados de esta manera, forman parte de la Carta de los Derechos Fundamentales de la Unión Europea, en los artículos 7, 8 y 11:

"Artículo 7. Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones

Artículo 8. Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente

Artículo 11. Libertad de expresión y de información.

[117] Directiva 95/46/CE

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2. Se respetan la libertad de los medios de comunicación y su pluralismo".

Cuando se trata de delimitar el ámbito de aplicación material de la propia Directiva sobre protección de datos, entonces el Tribunal de Justicia de la Unión Europea se posiciona claramente, según Castro (2015), a favor "únicamente de los derechos de las personas cuyos datos se encuentran en Internet, no prestando especial consideración a la libertad de información" (al estimar el Tribunal de Justicia que la actividad del motor de búsqueda se debe considerar como un tratamiento de datos frente al argumento de Google Spain y Google Inc. quienes mantienen que no existe tal tratamiento pues los motores funcionan con la información disponible en la red y no distinguen entre aquello que son datos de carácter personal frente a cualquier información de otra índole).

Parikh y Huniewicz (2015) abarcan varias de las fuentes de información relativas a *eHealth*, y los usos que los pacientes hacen de Internet, redes sociales, aplicaciones móviles, y páginas web. Por otro lado, Fernández-Luque y Bau (2015) sostienen que las redes sociales tienen una influencia muy poderosa en las decisiones que se toman en el ámbito de la salud. Afirman que existe actualmente una cantidad de datos, sin precedentes, que son susceptibles de ser utilizados en salud pública, a partir de la combinación de datos procedentes de teléfonos móviles, HCEs, redes sociales, y otras fuentes (el título de su artículo lo dice todo: "*health & social media, perfect storm of information*"); identificar información significativa, sustanciosa y útil, a partir de esas fuentes de datos no es fácil, más aún, se precisan nuevas herramientas de análisis que se tendrán que desarrollar en el futuro para estudiar esas fuentes de datos de forma que puedan beneficiar tanto a profesionales como autoridades sectoriales.

Bonneau y Preibusch (2010) ya detectaron que a pesar de la existencia de prácticas de seguridad deficientes, existe evidencia de que las redes sociales están haciendo esfuerzos para implementar tecnologías que mejoren la privacidad, con una mayor amplitud en la cantidad de controles que ofrecen en lo relativo a la privacidad. Sin embargo, muy acertadamente desde mi punto de vista, destacan que **la privacidad se utiliza raramente como un aspecto positivo desde el punto de vista comercial**, y en algunos casos sólo como una característica secundaria, pero no decisiva; las redes sociales tampoco han promovido controles de privacidad dentro de sus propias redes. Si identificaron gran diversidad en la longitud y el contenido de las políticas de privacidad, pero con una tendencia hacia la promoción más bien opuesta, pues casi todas las políticas se hacen inaccesibles a ojos de los usuarios más ordinarios debido al complejo lenguaje jurídico empleado. Estos autores llegan a la conclusión de que el mercado de la privacidad en las redes sociales es disfuncional, ya que hay una variación significativa en los controles de privacidad de los sitios, los requisitos

de recopilación de datos y las políticas de privacidad, pero esto no se comunica de forma efectiva a los usuarios. Sus hallazgos les animan a hablar de un novedoso modelo de "juego de comunicación de privacidad", donde la opción más racional, desde el punto de vista económico, para los operadores de redes sociales, es facilitar el acceso al control de privacidad, para evitar así las críticas de los "fundamentalistas" de privacidad, a la vez que se oculta el interfaz de control de privacidad y la política de privacidad, para maximizar las altas y animar a compartir al intercambio de datos de una mayoría de usuarios que se pueden consideran pragmáticos.

Si hablamos de webs de *eHealth*, nos podríamos imaginar una biblioteca con libros de salud, un número enorme de artículos que podemos consultar libremente...sin necesidad de esperar a la cita con un médico o profesional sanitario al cabo de varias semanas o meses. Pero más aún, no existen bibliotecarios al uso en Internet, a los que recurrir para encontrar la información que buscamos, o mejor dicho, si existen; se trata de los buscadores. Pero cuando identificamos algunas webs de interés, que se presentan de acuerdo a las preferencias del buscador, aparece la información que buscamos y nos encontramos, junto a artículos serios y rigurosos, algunos que no lo son, incluso con publicidad engañosa. En todo este azaroso proceso hemos ido dejando un rastro detallado de la información que estamos buscando, y si introducimos datos personales de salud, será información debe ser considerada como sensible.

Para valorar la fiabilidad de la información sobre salud que facilitan las páginas web y el posible tratamiento de datos de carácter personal hay que tener en cuenta que desde cualquier ordenador personal con un módem es fácil crear una página web, lo que no significa que ofrezca garantías. El código de conducta de la Fundación HON incluye ocho principios para garantizar la confianza de la información médica y de salud de las páginas web, uno de los cuáles se refiere a la confidencialidad[118]. Estos principios sirven para valorar si una página web ofrece la calidad necesaria, y esto no sólo implica identificar las fuentes de la información, sino respetar y exceder los requisitos de privacidad de la información.

Cómo decíamos Gertner (2010) cree que Internet y las redes sociales pueden ser herramientas muy útiles para realizar investigación de mercado y marketing; su afirmación la podemos poner en relación con lo que señala Wikipedia: "el software germinal de las redes sociales parte de la teoría de los seis grados de separación", de acuerdo al cuál todos los individuos del planeta están conectados entre sí a través de no más de seis personas. De hecho, existe una patente en EE.UU. conocida como "*six degrees patent"* por la que ya ha pagado LinkedIn. Hay otras muchas patentes que protegen la tecnología para automatizar la creación de redes y las aplicaciones relacionadas con éstas. Estas redes se basan en la teoría de los "seis grados de separación" según la cuál cualquier ser en la tierra puede estar conectado a cualquier otra persona en el

[118] "Este sitio web respeta la confidencialidad de los datos relativos a pacientes y visitantes, incluyendo su identidad personal. Los propietarios de este sitio web se comprometen a respetar y exceder los requisitos legales de privacidad de la información médica o de salud que se aplican en los países donde estén localizados tanto el sitio principal como sus réplicas (mirrors)" (https://www.healthonnet.org/HONcode/Spanish/).

planeta a través de una cadena de conocidos que no tiene más de seis intermediarios; las redes sociales han existido desde el comienzo de los tiempos, o más bien desde que existe la raza humana; la investigación sobre ellas queda evidenciada en la teoría de los seis grados (Llanos y Troncoso, 2016; Watts, 2004; Karinthy, 1930) y El Problema del Pequeño Mundo (Milgram, 1967); el psicólogo estadounidense Stanley Milgram ideó una nueva manera de probar la teoría, que él llamó "el problema del pequeño mundo". El experimento del mundo pequeño de Milgram consistió en la selección al azar de varias personas del medio oeste estadounidense para que enviaran tarjetas postales a un extraño situado en Massachusetts, situado a varios miles de millas de distancia. Los remitentes conocían el nombre del destinatario, su ocupación y la localización aproximada. Se les indicó que enviaran el paquete a una persona que ellos conocieran directamente y que pensaran que fuera la que más probabilidades tendría, de todos sus amigos, de conocer directamente al destinatario. Esta persona tendría que hacer lo mismo y así sucesivamente hasta que el paquete fuera entregado personalmente a su destinatario final. Aunque los participantes esperaban que la cadena incluyera al menos cientos de intermediarios, la entrega de cada paquete solamente llevó, como promedio, entre cinco y siete intermediarios. Los descubrimientos de Milgram fueron publicados en "Psychology Today" e inspiraron el término "seis grados de separación".

El origen de las redes sociales en la era de las TIC se produce, a más tardar, en 1995, cuando Randy Conrads crea el sitio web *classmates.com*; con esta red social se pretende que sus miembros puedan recuperar o mantener contacto con antiguos compañeros del colegio, instituto, universidad, etcétera. Con el nacimiento de Internet y la *world wide web*, se abrieron las puertas a las SNS; en 2002 comienzan a aparecer sitios web promoviendo las redes de círculos de amigos en red cuando el término se empleaba para describir las relaciones en las comunidades virtuales, y se hizo popular en 2003 con la llegada de sitios tales como LinkedIn o Xing. Friendster fue la primera red social en aparecer en 2002, más tarde la estructura de Friendster fue replicada por MySpace en 2003, Facebook en 2004 y Twitter en 2006. Friendster ha sido uno de los que mejor ha sabido emplear la técnica del círculo de amigos (Álvarez, 2012). La popularidad de estos sitios creció rápidamente y las grandes compañías han entrado en el espacio de las redes sociales en Internet, para explotar todas las oportunidades que ofrece, incluida la analítica de datos (Aguilar 2016). Las redes sociales continúan avanzando en Internet a gran velocidad, especialmente dentro de lo que se conoce como Web 2.0 y Web 3.0; y dentro de ellas, hay que mencionar un nuevo fenómeno destinado a ayudar al usuario en sus compras en Internet: las redes sociales de compras. Estas redes sociales de compras intentan abrirse camino como lugar de consulta y adquisición; un espacio en el que los usuarios no sólo pueden adquirir productos, sino donde también pueden consultar dudas sobre los productos, leer opiniones, escribir sus propias opiniones, e interactuar en general con otras personas con sus mismas aficiones; esta tendencia tiene nombre, se llama Shopping 2.0.

Algunos autores como Mayer y Leis (2010) destacan las oportunidades que abre la Web 3.0, con entornos 3D que pueden comprender centros de salud virtual, donde se plantean si actuaríamos igual que lo haríamos en la vida real o "como en un videojuego, de una forma más sencilla y sin la necesidad de disponer de capacidades especiales para su ejecución, citando como ejemplo el desarrollado por la Sociedad Española de Medicina de Familia en Second Life llamado “La isla de la salud” y en el que podemos encontrar incluso una consulta médica virtual” (ver figura 2.5.). Queda por investigar las numerosas utilidades que ofrecen este tipo de entornos pero parece que nos enfrentamos a un mundo de posibilidades en el sector de la salud, para usuarios de Internet en general, para los pacientes, para los profesionales sanitarios etcétera, pues se trata de una nueva herramienta, tal vez complementaria, para la realización de actividades de formación y educativas, de consulta virtual, de realización de estudios, de promoción de la salud para su posterior aplicación en la vida real.

Figura 2.5.
consulta médica en Second Life de la Sociedad Española de Medicina de Familia

Fuente: Mayer y Leis (2010)

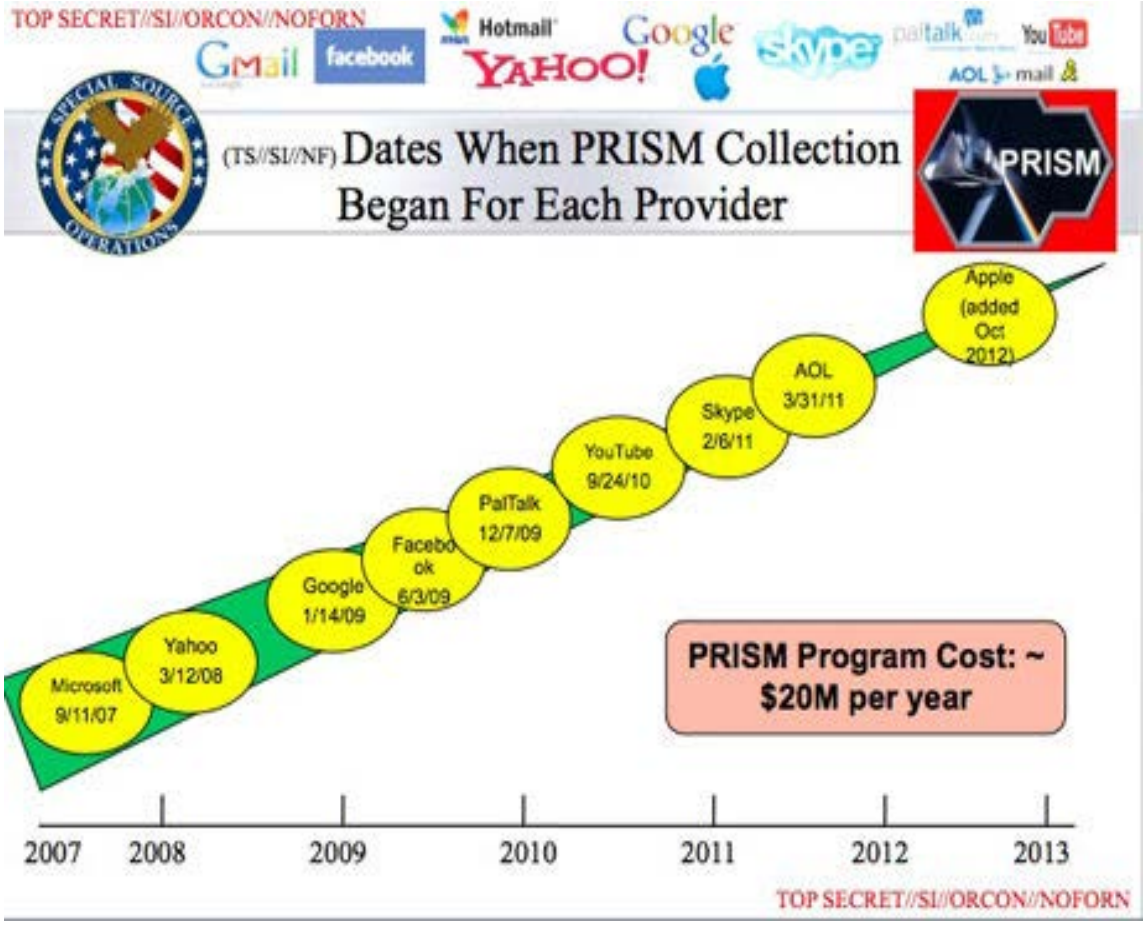
Estas nuevas plataformas, como las redes sociales, son una herramienta óptima para la comunicación entre individuos, pero sería muy ingenuo pensar que sólo sirven como la comunicación entre usuarios; así,

las compañías que almacenan ese volumen ingente de datos (Big Data), aprovechan la minería de datos, su análisis, para sacar el máximo aprovechamiento de los mismos con fines comerciales.

Según Rincón (2016) el capital, las empresas y los gobiernos parecen estar triunfando; los gobiernos están próximos al control total de los datos sobre los individuos (y en consecuencia de la sociedad). Ignoramos que nos persiguen y conocen nuestras intimidades conectadas a redes, sistemas, etcétera; incluso algunos (o no tan pocos) parecen felices entregados a la vigilancia y el control. Rincón habla pues de pasar **del optimismo tecnológico (donde el Big Data es sólo una tecnología -un invento que lo puede todo-), a la ironía de la tecnología (como dispositivo de poder) y al cinismo (del Big Data como ideología)** y de asumir que cada vez es más difícil reconocer que las redes digitales son un lugar democrático, porque estas redes agregan personas y datos a cuentas, pero no crean sociedad sino mas bien excluyen a aquellos que no están conectados y a los que no piensan igual, pero por otro lado además los miembros de esas redes están siendo controlados y vigilados; ver figuras 2.6. y 2.7.

Edward Snowden ha revelado el trabajo de la NSA y el programa PRISM. El programa PRISM permite a la NSA, la organización de vigilancia más grande del mundo, obtener comunicaciones específicas sin tener que solicitarlas al proveedor del servicio, y sin necesidad de tener que obtener órdenes judiciales (Greenwald y MacAskill, 2013). Este programa permite acceder a datos de usuarios de proveedores; la participación de proveedores de servicios de Internet en PRISM tales como Microsoft, Google, Yahoo, Facebook, Youtube, Skype, AOL y Apple (figura 2.6.), añade si cabe preocupación sobre el alcance de la vigilancia de la que los ciudadanos podemos ser objeto.

Figura 2.6.
Programa PRISM de la NSA,
fechas de inicio de la recogida de datos por empresas colaboradoras.



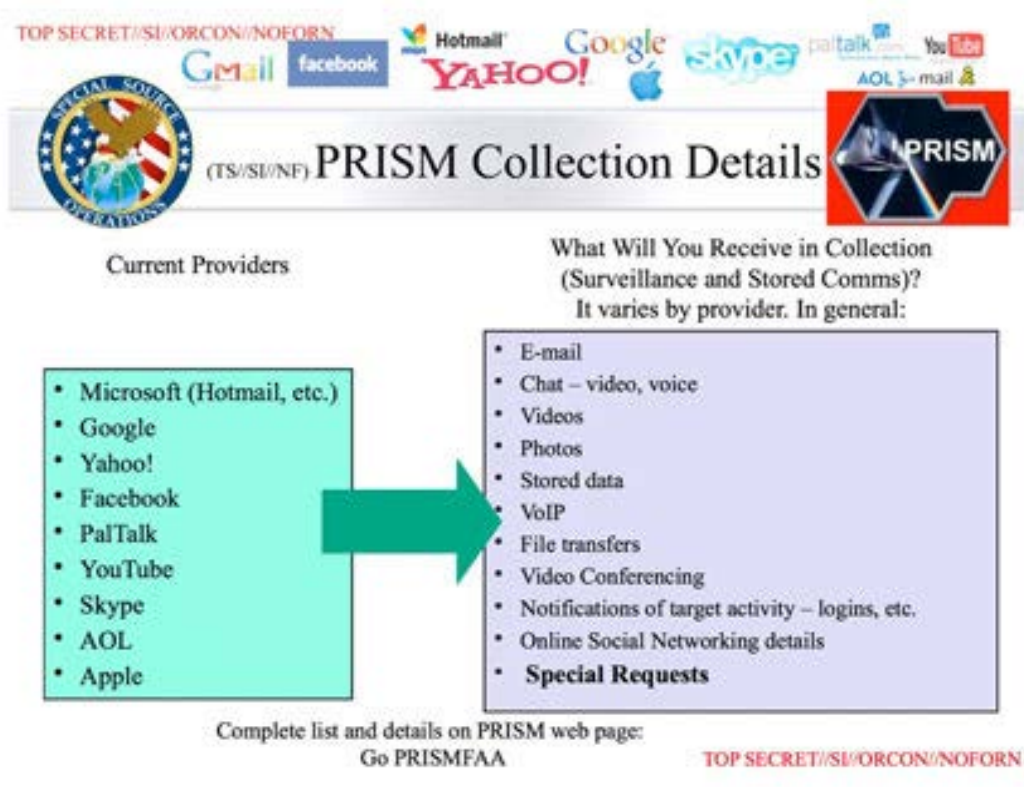
Fuente: documento secreto de la NSA publicado por The Guardian el 6 de junio de 2013.

Algunos de los proveedores de servicios de Internet más grandes del mundo son parte del programa desde su introducción en 2007, entre ellos Microsoft (que paradójicamente ha llevado a cabo una campaña publicitaria con el lema **"Tu privacidad es nuestra prioridad"**) fue el primero, seguido por Yahoo en 2008; Google, Facebook y PalTalk en 2009; YouTube en 2010; Skype y AOL en 2011; y Apple, que se incorporó en 2012. En su conjunto, tal y como recoge la figura 2.7., las compañías participantes cubren una gran mayoría de los servicios de correo electrónico, buscadores, intercambio de videos y redes sociales. Las empresas están legalmente obligadas, de acuerdo con la ley de EE.UU., a cumplir con las solicitudes de acceso a las comunicaciones de los usuarios de dichas empresas, pero con este programa la NSA puede acceder directamente a los servidores de las empresas participantes y obtener tanto las comunicaciones almacenadas, como realizar recopilación de datos en tiempo real; la figura 2.7. contiene un documento secreto de la NSA obtenido por The Guardian[119], y destaca el amplio expectro de datos a los que la NSA

[119] Recuperado de https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Último acceso 2 enero 2017.

puede acceder: correo electrónico, vídeo y chat de voz, vídeos, fotos, voz a través de IP (Skype, por ejemplo), chats, transferencias de archivos, detalles de redes sociales y mucho más.

Figura 2.7.
Proveedores de la NSA y servicios de vigilancia.



Fuente: documento publicado por The Guardian de la NSA de abril de 2013 relativo a la recogida de datos del programa PRISM.

La divulgación del programa de PRISM siguió a una filtración a *The Guardian* de una orden judicial secreta que obligaba al proveedor de telecomunicaciones Verizon a entregar los registros telefónicos de millones de clientes (Greenwald, 2013). A diferencia del acceso a registros de llamadas, la vigilancia de PRISM puede incluir el contenido de las comunicaciones, y no sólo los metadatos[120].

Como revelan Greenwald y MacAskill (2013) el documento "*top secret*" de la NSA indica que se está planeando agregar Dropbox como proveedor de PRISM; la agencia también busca ampliar los servicios

[120] Según Howe (1993) el término metadato, acuñado por Jack Myers en la década de los 60, se utiliza para describir conjuntos de datos. La primera acepción que se le dio fue la de dato sobre el dato (que proporciona la información mínima necesaria para identificar un recurso). El término no ha evolucionado en gran medida desde esta fecha, aunque sí lo han hecho los conceptos asociados a él, las aplicaciones y el nivel de uso de los metadatos (recuperado de http://www.sedic.es/autoformacion/metadatos/tema1.htm, último acceso 25 noviembre 2016).

de acceso a datos de los proveedores actuales. Parece bastante sorprendente que **la NSA esté solicitando a compañías privadas proveedoras de servicios que faciliten este acceso**; la NSA forma parte del ejército de los EE.UU. y por ello se puede decir que se ha concedido a los militares acceso sin precedentes a comunicaciones de civiles; se trata de una **militarización sin precedentes de la infraestructura de comunicaciones privadas**, lo cual es tremendamente preocupante cuando se defiende la separación de vida civil y actividad militar, la independencia, la libertad y la democracia.

Esta gravísima situación llevó a la Resolución del Parlamento Europeo, de 29 de octubre de 2015[121], sobre el seguimiento de otro acuerdo previo, la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la **vigilancia electrónica masiva** de los ciudadanos de la UE[122], que recoge el siguiente paquete de medidas de protección de datos (9 a 11):

"9. Acoge con satisfacción el inicio de negociaciones interinstitucionales informales sobre el proyecto de Reglamento general de protección de datos así como la adopción, por parte del Consejo, de una orientación general sobre el proyecto de Directiva sobre protección de datos; reitera su intención de concluir las negociaciones sobre el Paquete de medidas sobre protección de datos en 2015;

10. Recuerda al Consejo su compromiso de respetar la Carta de los Derechos Fundamentales de la Unión Europea en sus enmiendas a las propuestas de la Comisión; reitera, en especial, que el nivel de protección ofrecido no debe ser inferior al que se había fijado ya en la Directiva 95/46/CE;

11. Destaca que tanto el Reglamento de protección de datos como la Directiva sobre protección de datos son necesarios para proteger los derechos fundamentales de las personas y, por lo tanto, ambos deben tratarse como un paquete que se ha de adoptar de manera simultánea, con el fin de garantizar que todas las actividades de tratamiento de datos en la UE ofrecen un elevado nivel de protección en todas las circunstancias; subraya que el objetivo de reforzar los derechos y la protección de las personas en lo que respecta al tratamiento de sus datos personales debe cumplirse al adoptar el paquete;"

En estas circunstancias Rincón (2016) se refiere al conflictivo contexto actual de los datos como la "guerra de los datos". Estos datos que almacenan los proveedores de servicios son por tanto empleados con distintos fines (como acabamos de ver todavía hoy desconocidos en la mayoría de los casos, pues pueden tener consecuencias presentes o a futuro). Lo mismo sucede con compañías (privadas o públicas) que acceden a nuestros datos con fines comerciales (o de marketing) o que venden ciertos datos a terceros, poniendo en duda el respeto a las leyes sobre privacidad; Julian Assange y las revelaciones de Wikileaks con filtraciones de información han abierto los ojos al revelar las intimidades del mundo diplomático donde las guerras priman como un negocio, Snowden ha sacado a la luz la vigilancia masiva sobre los ciudadanos y el

[121] Parlamento Europeo. Resolución del Parlamento Europeo, 29 de octubre de 2015. Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//ES. Último acceso 24 diciembre 2016.

[122] 2015/2635 (RSP).

caso Falciani nos ha recordado que el capital es más valioso que las personas (la lista Falciani es como se identifica el caso de revelación de información de más de 130.000 evasores fiscales que Hervé Falciani sustrajo de la filial suiza del banco HSBC y que ha servido en diversos países para destapar casos de evasión fiscal). Así, capital y política van de la mano como si de una historia de amor se tratara (y así lo define Rincón), una relación estrecha entre administraciones (gobiernos) y organizaciones (empresas), donde la clave del amor son los datos; las administraciones aprueban leyes y vigilan en nombre de sus intereses y la seguridad nacional, y las empresas vigilan y controlan en nombre de sus accionistas en bolsa. Es una estrategia de negocio que obtiene capital y poder de los datos (Big Data), una sociedad que, como afirma Jorge Carrión (2015), ha evolucionado del Gran Hermano al Big Data como una peligrosa violación de **principios como el anonimato, la privacidad, la intimidad**.

Del análisis de las redes sociales y su aplicación a Internet, se puede concluir que están estrechamente relacionadas con el comportamiento, influencia, imagen, productividad, conducta, resultados y en relación con varios sectores como antropología, geografía, o economía; de acuerdo con Moreno Reyes (2015) España es uno de los países líderes en el uso de redes sociales y Twitter es la red líder de microblogging; también Twitter es la tercera red social más utilizada en España y la tercera red social preferida para ser utilizada en el futuro. Twitter actualmente está creciendo a un promedio anual del 33%; Su objetivo es obtener perfiles de ocio / profesionales basados en perfiles personales / profesionales y de microblogging. Twitter es una red social abierta con nivel horizontal de integración. Las nuevas herramientas de la tecnología de la comunicación (SMS o el sistema de mensajes cortos), Internet (Web 2.0), redes sociales...hacen que la comunicación sea más flexible en una dirección o más directa (Anduiza, 2009; Gibson, Ward y Lusoli, 2002), una evolución de la comunicación de uno a muchos (Gibson y Rommele, 2008), con sencillez del mensaje (Mylona, 2008), para promover la eDiscusión o discusión en la red (Bimber, 2001).

Dentro de Democracy 2.0. y Government 2.0 (Domínguez, 2009), las nuevas herramientas de la tecnología de la comunicación están en Internet, las redes sociales; las redes sociales promocionan la democracia digital o eDemocracia (Demertzis, Diantaki, Gazi y Sartzetakis, 2005). Twitter es una red social cuyo modelo de negocio se basa en la publicidad y la venta de sus datos a terceros, con fines comerciales y de marketing. El análisis de esta red social, con sus mecanismos, algoritmos, métricas, técnicas es una fuente con un enorme potencial para medir tendencias de comportamiento, gustos, y hacer predicciones, también sobre posibles epidemias.

2.4.3. Internet y los sitios web.

Al margen de las redes sociales, existen cada día un mayor número, indeterminado, de sitios web dedicados a la salud, con un número de funciones para interactuar con el paciente, y que van en aumento. Kim (2016) analiza el grado de confianza que generan estos sitios web, y concluye que la calidad de la información es un factor clave para determinar la confianza en las mismas por los usuarios y **consumidores**. Hueasch (2013) por su parte confirma que la privacidad difícilmente queda garantizada, pues es dícil que las búsquedas, (incluidos los temas de salud), queden en el anonimato, debido a la dirección de IP, las cookies, etcétera; defiende que **el anonimato está en peligro ante la visibilidad de Internet**, su transparencia; sus conclusiones determinan que los pacientes y los médicos que estén preocupados seriamente por la privacidad de la información sobre sus búsquedas relacionadas con la salud, suelen buscar información en sitios web del gobierno o de las sociedades profesionales, a la vez que invita utilizar herramientas de privacidad, disponibles de forma gratuita, para buscar y navegar por Internet (por ejemplo, DoNotTrackMe y Ghostery). En caso de que los sitios web dedicados a la salud no sean capaces de garantizar la privacidad, ello repercutirá en la confianza de los usuarios. Sólo mencionar aquí algunos de los sitios web sobre salud más populares (mayoritariamente en inglés y con origen en EE.UU.) que conviene citar[123], varios de los cuales son efectivamente gubernamentales:

-*Centers for Disease Control and Prevention* (http://www.cdc.gov). CDC es parte del departamento de salud de los EE.UU., y tiene por objetivo prevenir y controlar las enfermedades, lesiones e incapacidades. Es una de las mejores páginas web del gobierno, que abarca desde enfermedades como el ébola al sida. Con una muy amplia cobertura, también facilita información en español.

-*The Cleveland Clinic Health Information Center (*http://my.clevelandclinic.org/health/default.aspx). Web de la Clínica Cleveland para beneficio de pacientes, el público en general y los profesionales sanitarios. Hay un chat en vivo de lunes a viernes y un centro de enseñanza *online* para mejorar el conocimiento sobre enfermedades y tratamientos, y hasta se puede realizar un chequeo de síntomas.

-*Familydoctor.org (*http://familydoctor.org/familydoctor/en.html) El contenido de esta web está destinado a individuos que buscan información de salud que sea fiable. Las enfermedades se pueden buscar por nombre, síntomas o edad más común de los afectados.

[123] La página web Caphis *(*"*consumer and patient health information section"*) recoge un listado muy completo (http://caphis.mlanet.org) llamado "*Top 100 List: Health Websites You Can Trust", aquí incluimos sólo una muestra.*

-*Healthfinder (*http://www.healthfinder.gov/). Gestionado por el departamento de salud, facilita información fiable de unas 1.400 organizaciones de salud. Ofrece herramientas para encontrar servicios de salud y atención, también en español.

-*Mayo Clinic (*http://www.mayoclinic.com). Está considerada unas de las mejores instituciones hospitalarias de EE.UU. y una de las más reconocidas del mundo en las especialidades de ortopedia, neurocirugía, cardiología y cáncer. La Clínica Mayo es una entidad sin ánimo de lucro dedicada a la práctica médica desde su fundación en 1889. Su sede es la Mayo Medical School y sus instalaciones para la investigación están en Rochester, Minnesota. Ofrece información médica y de salud fácil de entender, además de ofrecer chequeo de síntomas y blogs de expertos.

-*MedlinePlus (*http://www.medlineplus.gov). Se trata de una web creada y mantenida por la *National Library of Medicine*, parte del *National Institutes of Health*, para asistir a consumidores y usuarios a localizar información de salud fiable. Incluye sesiones interactivas para formar a los pacientes. Ofrece servicios en más de 40 idiomas, incluido el español.

-*Merck Manual Home Edition for Patients and Caregivers (*http://www.merckmanuals.com/home/index.html). Basado en el libro de medicina ampliamente utilizado, la edición *online* del Manual Merck se escribe en un lenguaje sencillo, e incluye tests médicos.

-*NetWellness (*http://www.netwellness.org) Se trata de una web de salud sin ánimo de lucro. Facilita más de 55.000 páginas de alta calidad, creadas y evaluadas por médicos y profesionales de la Universidad de Cincinnati, la Universidad Case Western Reserve, y la Ohio State University. Tiene una característica muy interesante, "*Ask An Expert*", un servicio de pregunta y respuesta facilitado por profesionales de las tres universidades.

Cole, Watkins y Kleine (2016) en su estudio sobre sitios web de salud concluyen que la mayor parte de la información evaluada de dichos sitios web (que fue valorada por médicos cualificados y encuestados no cualificados como médicos) era de una calidad razonablemente aceptable, aunque una pequeña cantidad de la información evaluada fue considerada como pobre, por lo tanto sugieren que los foros de discusión pueden ser una plataforma útil a través de la cual los usuarios pueden hacer preguntas relacionadas con la salud y recibir respuestas de calidad aceptable.

Sin embargo existen visiones muy distintas, como la defendida por Sugiyama (2016), cuyo trabajo recoge datos sobre cómo los ciudadanos utilizan los buscadores de manera frecuente para tratar de encontrar información sobre su estado de salud, situación que conduce al autodiagnóstico, lo cuál resulta espcialmente

preocupante cuando más tarde acuden al hospital y reciben un tratamiento tardío, precisamente debido a un **erróneo autodiagnóstico del paciente (y posiblemente acompañado de una incorrecta automedicación).**

Por ello, existen entidades independientes que certifican la credibilidad y la fiabilidad de los sitios web, a través de la **concesión de sellos de calidad**, acreditación independiente que agiliza el proceso de validación para los usuarios[124], como por ejemplo:

-HONcode (*health on the net code*), concedido por la Health On the Net Foundation, organismo no gubernamental, sin ánimo de lucro, con sede en Ginebra, fundado en 1996, exige cumplir 8 principios de honradez y calidad, que incluyen la confidencialidad de los datos de salud[125]. Se trata de la fuente de acreditación de mejor valorada, con 20 años de experiencia, y la más veterana según Boyer et al. (2016).

-WMA (web médica acreditada), concedido por el Colegio de Médicos de Barcelona para la mejora de la calidad de la información sanitaria en Internet, es una programa calidad y de certificación de webs de contenido sanitario en España y América Latina, fundado en 1999, que exige cumplir con las buenas prácticas definidas por el propio Colegio, que incluye la monitorización de los sitios web y la confidencialidad[126].

[124] Mayer Pujadas (2006).

[125] HonCode. Recuperado de http://www.hon.ch/HONcode/Patients/Visitor/visitor.html. Último acceso 1 de enero 2017.

[126] Web Médica Acreditada. Recuperado de http://wma.comb.es/es/home.php. Último acceso 5 de enero 2017.

Capítulo 3. Análisis del modelo de protección de datos en la UE, *eHealth*.

Desde que se aprobó la Directiva 95/46/CE de protección de datos de carácter personal, la UE ha adoptado una serie de normas que han contibuído ha definir la manera en que se deben proteger los datos de carácter personal. Más de veinte años después se ha transformado la tecnología y con ella la forma de acceder a los datos, cómo se recogen y se procesan. En este capítulo se abordan los elementos integrantes del modelo europeo, donde los 28 Estados miembros han transpuesto el contenido de esa Directiva.

El resultado ha sido un régimen regulatorio homogéneo pero dispar, con ciertas divergencias en la aplicación de dichas normas. Esta disparidad ha llegado a convertirse en una **costosa carga administrativa para las empresas**, ante la ausencia de un marco jurídico uniforme, según defienden Bäumer, von Oelffen y Keil (2017), especialmente ante el desarrollo del IoT, donde los dispositivos conectados a Internet recogen una gran cantidad de datos, y esto supone una serie de obligaciones para las empresas en cada país donde operan. Este hecho y la **necesaria conciliación entre seguridad y privacidad**, han contribuido a la evolución del marco de protección de datos de la UE, en un contexto donde la tecnología está cambiando rápidamente (a través de dispositivos móviles), con nuevas soluciones también en el campo de la salud, dejando obsoletes muchas normas en vigor.

Se analizan en este capítulo por un lado las actitudes sobre la protección de datos e identidad electrónica de los ciudadanos europeos, y por otro se compara la cultura sobre datos de carácter personal hacia la adaptación a un marco legal armonizado, donde el motor de este modelo es el propio ciudadano europeo.

3.1. Introducción.

Los derechos fundamentales se vienen consolidando a nivel internacional como emanación de la dignidad humana y existe la necesidad de un efectivo respeto a los derechos fundamentales del individuo en cualquier Estado constitucional de derecho (Alcalá, 2016; Machado, 2015).

El establecimiento de principios éticos se ha hecho más necesario que nunca ante la evolución de la ciencia y la tecnología; el artículo 9 de la Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO aprobada el 19 de octubre de 2005[127] establece que la privacidad de las personas y la confidencialidad de la información que les incumbe deberían respetarse al abordar cuestiones éticas en relación a la medicina, las ciencias de la vida y las tecnologías (Buisán y Sánchez Urrutia, 2011).

[127] La UNESCO en su portal recuerda: "Esta declaración responde a una verdadera necesidad a medida que se multiplican, a menudo sin un marco regulador, prácticas que traspasan las fronteras nacionales: la realización simultánea en diferentes países de proyectos de investigación y de experimentos en el campo biomédico, la importación y exportación de embriones y células madre embrionarias, de órganos, de tejidos y de células, y la circulación transfronteriza de tejidos, de muestras de ADN y de datos genéticos" (http://portal.unesco.org/es/ev.php-URL_ID=30274&URL_DO=DO_TOPIC&URL_SECTION=201.html

Así todo, muchos países han iniciado desde el siglo pasado una titánica lucha por alcanzar dicho objetivo. Se han logrado grandes avances, especialmente en el seno de la UE, pero hay que superar las barreras para conseguir una plena igualdad y efectiva libertad individual, si es que este objetivo es posible de alcanzar.

Vivimos la eclosión del IoT, y con ello pronto todos los dispositivos que tenemos (o podamos imaginar) estarán conectados a Internet; según la consultora tecnológica Gartner Inc. se prevé que 2016 habrá finalizado con un 30% más de dispositivos conectados que el año anterior, y que en el año 2020 se multiplique por tres (Gasiorowski-Denis, 2016)[128]; en 2020 se espera que más de la mitad de los sistemas de negocio y procesos principales hayan incorporado algún elemento del IoT; así se puede afirmar que **el IoT tiene poder para transformar el mundo que conocemos**, aunque estamos en los inicios de dicha transformación, en el camino hacia la conectividad máxima. Ahora más que nunca se hace necesario un modelo de protección de datos de carácter personal, que permita adaptarse a los nuevos entornos.

3.2. Big Data en *eHealth* y privacidad.

Brynjolfsson y McAfee (2012) analizan cómo la revolución digital acelera la innovación y está transformando la economía de forma irreversible. En este apartado se abarca el concepto de Big Data, en el contexto de la salud digital, desde la perspectiva de la privacidad. A pesar de los rápidos avances del Big Data (Snijders, Matzat y Reips, 2012), hay que ponerlo en perspectiva, especialmente en un campo tan sensible como la salud, pues en él confluyen multitud de datos provenientes de numerosas y variadas fuentes.

El Big Data tiene un contenido informativo limitado según apuestan algunos investigadores (Kwan, 2016), debido a la influencia (que puede ser potencialmente significativa) de los algoritmos en los resultados de la investigación y al hecho de que **el conocimiento sobre el mundo generado con Big Data podría ser más un artificio de los algoritmos utilizados que de los datos en sí.** Baesens, Bapna, Marsden, Vanthienen y Zhao (2014) defienden que el Big Data y su analítica son el hilo conductor de cambio perturbador en el mundo empresarial en red. Sin olvidar la possible erosión de la privacidad y la pérdida de la dignidad humana a favor de imperativos económicos (Barocas y Nissenbaum, 2014). Se trata de evaluar la cadena de valor de la información que analizan en detalle Abbasi, Sarker y Chiang (2016), con el riesgo latente para el titular de los datos, el individuo, que no es consciente de cuánto y a dónde van a viajar sus datos, y sin que ni

[128] Artículo "Cómo cambiará nuestra vida con Internet de las Cosas" publicado por la Revista AENOR, procedente de ISOfocus, la revista de ISO bimestral, cuyos artículos publica la revista AENOR es seis de sus 11 números. ISOfocus contiene reportajes que pretenden mostrar los beneficios de la aplicación de las normas internacionales.

siquiera en el momento de la recogida del dato se conozca el valor que tendrá ese dato (Barocas y Nissenbaum, 2014). Resulta en este punto interesante recurrir al planteamiento de Han (2014), defendido por Vásquez Rocca (2015), que alerta de las políticas de la optimización personal, del rendimiento, y de la competitividad…que considera técnicas alabadas por la sociedad actual, con el fin de lograr la productividad ilimitada. Es precisamente esta dinámica a la que se someten los individuos, empujados a una **necesidad de constante optimización, que conduce a la paradoja de acabar generando en sí misma enfermedades** como la depresión, ansiedad, trastornos del sueño, insomnio, migrañas, etcétera. Curiosamente este sistema es el que acaba generando muchas de las enfermedades actuales que conducen un aumento del gasto en servicios sanitarios, bajas médicas, etcétera, para los estados y las empresas. Puede parecer este un planteamiento sesgado y poco ortodoxo, pero estos investigadores defienden una posición que creo es digna de un más profundo análisis. Si este régimen neoliberal que se ha implantado en el mundo occidental continúa generando dependencias de esta índole (como defienden con tesón y resignación dichos investigadores), y los grandes operadores de Internet persisten en su colaboración con organizaciones gubernamentales (como la mencionada NSA, ver figura 2.6. y 2.7.), **habrá que poner en cuarentena muchos de los planteamientos actuales respecto a la privacidad y la salud**; Han (2014) habla de esta sociedad del rendimiento en la que vivimos, donde el emprendedor ya no sufre tanto de enfermedades víricas sino neuronales (que identifica con la depresión, trastornos derivados de la hiperactividad y la fatiga neuro-funcional), consecuencia de apelar a la capacidad del individuo, y no tanto a la disciplina, en lo que ha calificado como el aparente tránsito de la coacción a la libertad del individuo[129].

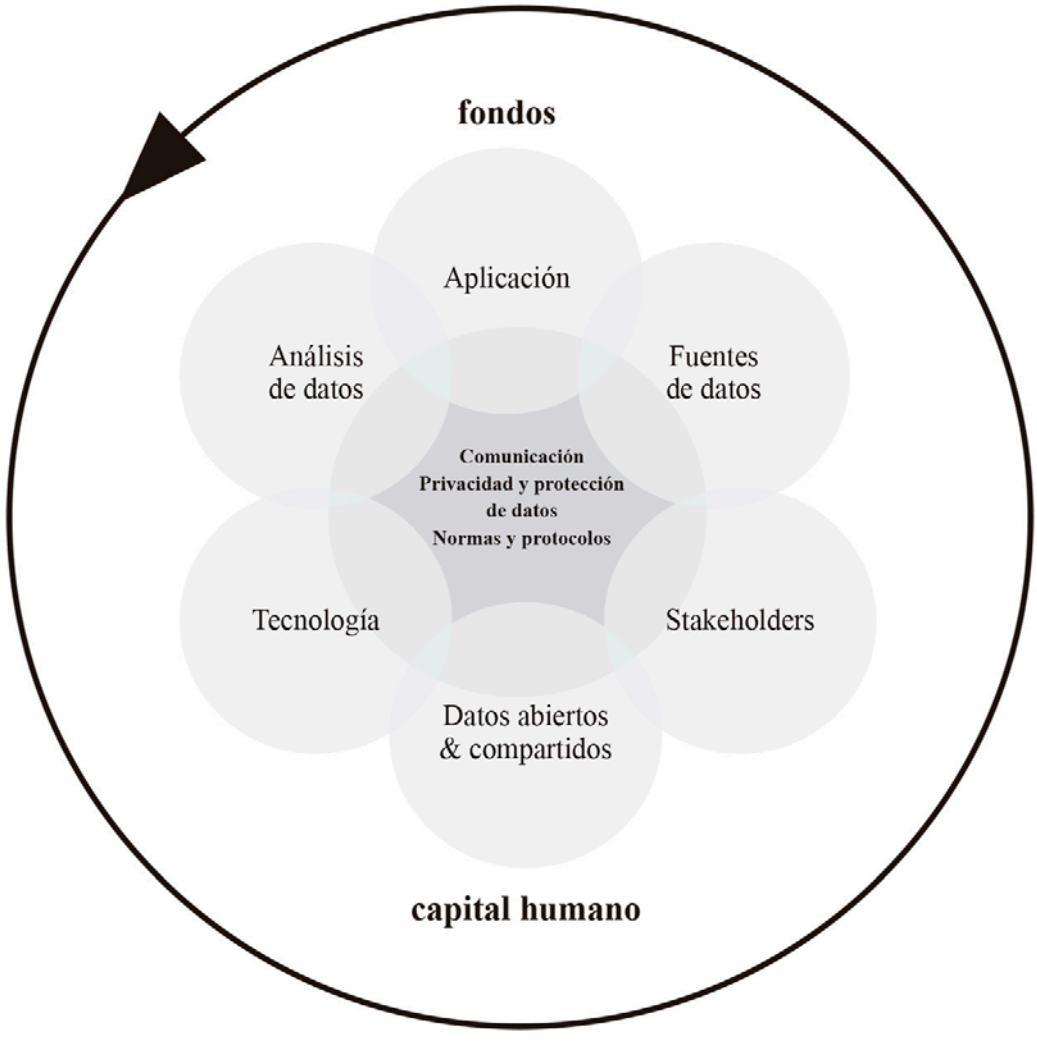
El Big Data está en una fase incipiente y afecta tanto a la vida íntima del individuo como a la seguridad de un país, así la enorme información que aporta ha mostrado su capacidad para que las organizaciones gubernamentales (no siempre de forma lícita) se sirvan de su desarrollo para la toma de decisiones; lo importante es extraer información fiable del Big Data que son datos inciertos y no estructurados, como señalan Singh, Mani y Singh (2016).

La UE ha trabajado en un nuevo marco regulatorio de protección de datos que tendrá aplicación a partir de 2018, con consecuencias directas sobre las empresas que trabajan con Big Data; los derechos de las personas deben quedar protegidos y el individuo debe poder tener la tranquilidad de que así será cuando emplee los nuevos instrumentos a su alcance en el entorno de *eHealth*, aunque algunos investigadores médicos reconocen que **proteger la privacidad de los datos del paciente resulta casi imposible** (Enserink y Chin, 2015).

[129] Vásquez Rocca analiza de forma promenorizada los planteamientos de Han en su artículo: "Byung-Chul Han: La sociedad de la Transparencia, Cansancio elocuente y Psicopolítica: De lo viral-inmunológico a lo neuronal-estresante", 2015.

En la figura 3.0. a continuación recojo los campos de acción (y sus interrelaciones potentciales) para el desarrollo de políticas de Big Data en salud, identificados en el marco de un acuerdo específico con la Agencia Ejecutiva de Consumidores, Sanidad y Alimentación (Chafea[130]) por mandato de la Comisión Europea[131]; se trata de los siguientes campos específicos (**situándose la protección de datos en el centro de todas las políticas**): los aspectos legales, los interesados, la privacidad y la protección de datos, los datos abiertos y compartidos, las normas y protocolos, el desarrollo tecnológico, las fuentes de datos, análisis de los datos, las aplicaciones, la comunicación, el capital humano, y la financiación -los fondos-.

Figura 3.0.
Visión general de los campos de acción en políticas de Big Data en salud y sus intersecciones potenciales



Fuente: elaboración propia a partir de información del *"Study on Big Data in Public Health, Telemedicine and Healthcare"* de la Comisión Europea, diciembre 2016.

[130] Acrónimo del inglés "*Consumer, Health and Food Executive Agency*".

[131] Comisión Europea. *"Study on Big Data in Public Health, Telemedicine and Healthcare"*, 16 diciembre 2016.

En este universo del Big Data destaca como efectivamente la privacidad y la protección de datos se sitúan en una posición de atención preferente en el marco de las políticas de Big Data en salud; se trata de un marco de actuación protector de grandes sistemas de datos y con incentivos para mejorar la privacidad de los datos. Se requiere consenso y la identificación de posibles lagunas en la protección jurídica, por lo que se recomienda redactar una política en materia de protección y seguridad de los datos personales, que sea integradora y coherente, que de acuerdo con el informe debe abordar: (1) normas para la propiedad y el control de los datos -es decir, que incluya cláusulas de exclusión- (2) especificación del propósito del uso de lo datos y limitación del uso (3) confidencialidad (4) acceso a los datos (tanto para pacientes como para profesionales de la salud) (5) servicios en la nube (6) almacenamiento y procesamiento de los datos, y un aspecto con importantes repercusiones (7) la reutilización y el flujo transfronterizo de datos[132].

Hay que tener en cuenta que una parte muy significativa de lo que hoy se llama Big Data es información sobre nosotros mismos, a la vez que a través de nuestra actividad electrónica dejamos un rastro de huellas digitales que revelan quienes somos, lo que compramos, a donde vamos, y mucho más. Llegan a la conclusión de que **una vez que los datos han sido recogidos no tenemos control alguno sobre quien los usa y cómo se utilizan** (Craig y Ludloff, 2011). El Presidente y cofundador de Sun Microsytems, Scott McNealy, dijo en 1999 que debemos resignarnos al hecho de no tener privacidad: *"You already have zero privacy. Get over it"* (Mañas, 2009; Solove, 2004). La protección de la privacidad implica hacer política y políticas públicas tanto como derecho y tecnología; en un mundo globalizado sin fronteras esto significa que **las políticas sobre privacidad hoy en día son interdependientes** (Bennett y Raab, 2006). Algunos investigadores creen que sólo con ejemplos de la vida real se puede justificar la necesidad de compartir datos para mejorar la atención sanitaria (Heitmueller, Henderson, Warburton, Elmagarmid y Darzi, 2014).

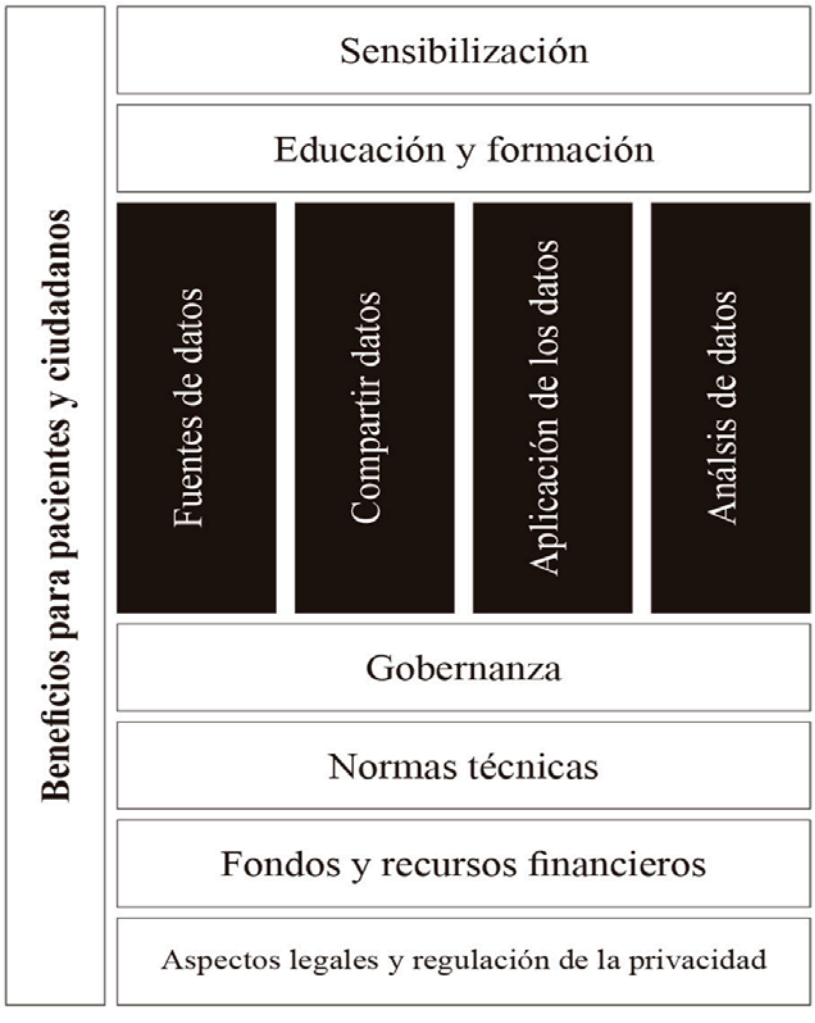
De hecho en 2006 el Comité de Ministros del Consejo de Europa estableció la celebración anual del Día de la Protección de Datos en Europa el 28 de enero, en conmemoración del aniversario de la firma del Convenio 108 del Consejo de Europa (para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal); por lo tanto, concienciar a la sociedad se presenta como una constante necesidad. Este reto es uno de los más importantes que se plantea este derecho fundamental a la protección de datos de carácter personal, que debe servir de garantía para que los individuos puedan controlar el uso de sus datos personales; el reconocimiento de este derecho fundamental forma parte del proceso de integración europea que hoy en día se está desarrollando, algo que ya defendía Ramiro (2006).

[132] Por todo ello se debe hacer hincapié en soluciones de seguridad de datos que sean nuevas e innovadoras; se deben adoptar los más altos estándares éticos (como, por ejemplo, un código para el análisis responsable), y se requiere desarrollar modelos de consentimiento polivalente que vayan dirigidos a los pacientes y titulares de los datos, especialmente en casos de investigación biomédica y genómica, para cumplir con todos los requisitos legales pero también éticos. Por otro lado se hace necesario un intercambio de datos con alta protección, a lo que puede contribuir la transparencia de la información sobre el uso de datos de salud, así como los incentivos para desarrollar tecnologías de privacidad -arquitecturas técnicas- (Comisión Europea. 16 diciembre 2016. *"Study on Big Data in Public Health, Telemedicine and Healthcare").*

El estudio comisionado por la Comisión Europea[133] realiza una serie de recomendaciones que tienen por objetivo proporcionar una serie de **directrices para el desarrollo de una cadena de valor de la UE de Big Data en al campo de la salud**. El Big Data en *eHealth* se refiere a grandes conjuntos de datos recogidos de forma rutinaria o automática, y que son capturados y almacenados electrónicamente. Comprende la fusión y conexión de bases de datos existentes con el propósito de mejorar la salud y el rendimiento de los sistemas de salud. Las recomendaciones que se presentan en la figura 3.1. a continuación (en su dimensión horizontal, vertical, y global) tienen por objetivo la mejora de la salud de los ciudadanos y pacientes europeos, a través de una mejora de los sistemas de salud de la Estados miembros; así pues, las recomendaciones están realizadas desde una perspectiva de salud pública. Ver apartados 3.4.1.1. a 3.4.1.10. donde se aborda cada recomendación con mayor grado de detalle.

[133] Comisión Europea. 16 diciembre 2016. *"Study on Big Data in Public Health, Telemedicine and Healthcare"*.

Figura 3.1.
Campos de recomendación de políticas en salud pública



Fuente: elaboración propia a partir de información del "*Study on Big Data in Public Health, Telemedicine and Healthcare"*, Comisión Europea, diciembre 2016.

Así todo, Craig y Ludloff (2011) creen que los datos de carácter personal son el activo más valioso hoy en día, más que el oro, pues los individuos representan el activo más deseado por empresas, industrias, ONGs y gobiernos. La tecnología digital está alimentando un nuevo orden mundial donde lo que antes era imposible ahora es posible. Tal vez no vivimos todavía en el mundo que George Orwell visionó en su novela 1984 (Orwell, 1990), un mundo sin derecho a la privacidad donde el gobierno controla a los ciudadanos. Pero hoy día los gobiernos usan nuestra información personal para su beneficio, resultando en un conocimiento mucho mayor sobre nosotros, que el que Orwell pudo nunca imaginar; el Gran Hermano suple a todo personaje político, es el comandante en jefe, el guardián de la sociedad, el dios pagano y el juez supremo. En una carta a un líder sindicalista estadounidense Orwell dijo sobre su novela 1984: "yo no creo que el género de sociedad que describo vaya a suceder forzosamente, pero lo que sí creo (si se tiene en cuenta que el libro es una sátira) es que puede ocurrir algo parecido. También creo que las ideas totalitarias

han echado raíces en los cerebros de los intelectuales en todas partes del mundo y he intentado llevar estas ideas hasta sus lógicas consecuencias". Palabras que nos hacen reflexionar, y especialmente concienciarnos de la trascendencia de la información que hoy día circula por Internet.

Garrie y Wong (2007) hacen un análisis de los datos de clics en cadena (Internet) desde una perspectiva europea y norteamericana, teniendo en cuenta el marco regulatorio, de protección de datos, en Europa (Directiva 95/46/CE de protección de datos de carácter personal; y la Directiva sobre la privacidad y comunicaciones electrónicas) y el marco jurídico de los EE.UU., en particular, la Ley Wiretap U.S.C. § 2701 (2004) y sus normas de desarrollo; examinan en qué medida los datos de los clics pueden considerarse datos de carácter personal de acuerdo con las normas de protección de datos, y cuáles son las consecuencias para los consumidores y las empresas.

Parte de la literatura habla de un conflicto de intereses, individuo versus colectividad; Ploem (2006) en su artículo *"Towards an Appropriate Privacy Regime for Medical Data Research"* valora la investigación médica y la intimidad como principios fundamentales que pueden entrar en conflicto. Aunque varias legislaciones europeas e internacionales regulan la privacidad en este ámbito, donde no existe una clara definición del concepto de datos encriptados, por ejemplo; en este artículo se señala cuál debería ser el régimen ideal de privacidad para la investigación con datos médicos; el autor cree que hay que aprobar un marco común europeo o internacional para la investigación con datos médicos y tejidos humanos, pues sin este marco la investigación médica transnacional nunca será realmente efectiva[134].

3.2.1. Protección de datos (UE) versus privacidad (EE.UU.).

Mientras los principios básicos para el trato justo de la información personal son comunes en todos los regímenes democráticos, los derechos que asisten a los individuos varían considerablemente de un país a otro; Reidenberg (2000) muestra que las diferencias entre regímenes radican básicamente en dos opciones políticas distintas, de acuerdo al modelo de sociedad democrática y los papeles asignados al Estado, al mercado y al individuo: ya sea el modelo liberal, basada en el libre mercado, o el modelo de gobernanza basado en la protección social y los derechos del individuo. Estas divergencias estructurales hacen imperativa la cooperación internacional para una protección eficaz de los datos en Internet. Si bien el análisis de Reidenberg en cuanto a los modelos de sociedad parecen acertados, desde el punto de vista de los derechos fundamentales, tan arraigados en la vieja Europa, no parece fácil una armonización entre los dos modelos.

[134] El artículo 27 de la Directiva sobre la privacidad y comunicaciones electrónicas 2002/58/CE Europea sobre Privacidad estipula que "*los estados miembros y la Comisión deben velar por el desarrollo de códigos de conducta que contribuyan a la adecuada implementación de las normas nacionales…teniendo en cuenta las características específicas de cada sector"*.

Las diferencias que existen entre Europa y EE.UU. no son nimias, tanto en el plano normativo como a escala ideológica; en Europa existe una tradición democrática de confianza en la protección del Estado, mientras **en EE.UU. la tendencia es limitar al máximo el papel del Estado**, cuya intervención queda reservada para materias concretas y situaciones excepcionales; se trata de dos visiones del estado ideológicamente diferentes.

De acuerdo con Hatfield (2016) se puede decir que el modelo norteamericano defiende la priorización de la seguridad sobre la privacidad o vida privada, pero también hay diferencias inherentes en la estructura básica del régimen estadounidense. Hatfield aboga por 3 diferencias básicas, que caracterizan el modelo de EE.UU.:

- Un sistema sectorial: las regulaciones para la protección de datos son determinadas de forma sectorial, sector por sector, y no dependen de un conjunto uniforme de regulaciones en todos los ámbitos, como ocurre en el sistema regulatorio de la UE. Este sistema ofrece flexibilidad, puesto que cada sector afecta a la privacidad de forma diferente, y del mismo modo, las preocupaciones por los datos de carácter personal de algunos sectores son mucho más sensibles que las de otros. Si se aborda el sector médico, por ejemplo, el sistema sectorial de los EE.UU. se concentra en situaciones en las que el abuso probablemente causará lesiones. La Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) de 1996 es un ejemplo de este modelo; se trata de un esquema de cumplimiento referido a los datos médicos de carácter personal que no se aplica a otro tipo de datos. En el marco del régimen de la UE, las normas aplican a todo tipo de datos. El efecto práctico de HIPAA es que los datos de carácter personal que son sensibles quedan protegidos y sólo pueden ser compartidos en casos específicos y limitados. De la misma manera que HIPAA elevó el grado de protección de ciertos tipos de datos, el sistema de EE.UU. ha reducido las protecciones para otros; entre estas reducciones en el grado de protección están la Ley de Vigilancia de Inteligencia Extranjera (FISA[135]) y las Cartas de Seguridad Nacional (NSL[136]).

- El efecto post-9/11: el método más común para que el gobierno de los Estados Unidos evite la regulación de la protección de datos es a través del uso de órdenes de búsqueda y de citaciones de gran jurado; la Cuarta Enmienda de la Constitución de EE.UU. estipula "*el derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"*. Esta enmienda también aplica a

[135] Acrónimo del inglés "*Foreign Intelligence Surveillance Act"*.

[136] Acrónimo del inglés "*National Security Letters"*.

la protección de los datos, defiende Hatfield, pues si se sigue el lenguaje empleado por la Cuarta Enmienda, los datos pueden ser sometidos a "*pesquisas y aprensiones*". Sin embargo, el gobierno no se limita a estos mecanismos cuando intenta confiscar datos y, a raíz del 11-S, sus poderes de búsqueda e incautación se expandieron considerablemente; la Ley PATRIOT amplió los poderes tanto de las NSL como de la FISA.

- Escepticismo de la UE: Para Hatfield los críticos del régimen estadounidense de protección de la privacidad han señalado a menudo que la protección de los EE.UU. respecto a los datos de carácter personal es "inadecuada" debido a la percepción de que los datos pueden ser arbitrariamente incautados y obtenidos, y que ciertos tipos de datos no reciben las mismas protecciones que los datos que el gobierno ha considerado "sensibles". Hasta cierto punto, estos detractores tienen una base sólida para su escepticismo, pues es cierto que los datos del extranjero, específicamente, han recibido menos protección; pues históricamente se han recogido, y se ha tenido acceso a ellos.

Los dos modelos (UE/EE.UU.) y sus diferencias están a la base del estado de bienestar que Navarro Ruvalcaba (2006) ha definido básicamente como "un conjunto de instituciones públicas proveedoras de servicios sociales, dirigidas a mejorar las condiciones de vida y a promover la igualdad de oportunidades de sus ciudadanos"; se trata de modelos de bienestar diferentes, donde el modelo de EE.UU. se caracteriza por una política liberal, una economía capitalista, y políticas sociales meramente residuales. El estado del bienestar estadounidense ha tenido tradicionalmente un carácter distintivamente descentralizado, como defiende Kagan (2007); históricamente desde los planes de pensiones de los empleados, pasando por los seguros de accidentes en el lugar de trabajo y hasta los servicios de atención sanitaria, se han dejado en manos del sector privado con que ha asumido mayor responsabilidad respecto a lo que ha sido el caso en el estado del bienestar europeo. Como los proveedores de estos beneficios y servicios en EE.UU. son numerosas entidades privadas, muchas de ellas compiten para reducir costes, por lo que los litigios en los tribunales, sobre los beneficios y coberturas, han sido mucho más comunes en los EE.UU. que en Europa.

Si abordamos la protección de datos, la distancia entre ambos lados del Atlántico representa la lejanía de las dos concepciones; mientras en Europa existe una concepción de protección de datos paternalista y (donde el ciudadano es el titular de sus propios datos) en EE.UU. predomina precisamente lo contrario, como refleja la siguiente comparativa[137]: la UE se rige por una Directiva y el nuevo Reglamento será de aplicación directa en todos los Estados miembros, actualmente las agencias nacionales en cada Estado miembro vigilan el cumplimiento de la normativa, que tiene un alcance general y preventivo, se protege a todo ciudadano en la UE, y sólo se recogen datos (en principio) cuando es necesario, se confía en

[137] Plaza, E. Comparativa de la Protección de Datos en Europa y en Estados Unidos. Recuperado de http://www.eljurista.eu/2015/04/26/comparativa-de-la-proteccion-de-datos-en-europa-y-en-estados-unidos/. Último acceso 10 octubre 2016.

la protección del Estado, y las sanciones están tasadas al margen de la vía penal; en el caso de EE.UU. sólo existen normativas sectoriales, no hay normativa constitucional de alcance general, tampoco existe agencia alguna o autoridad específica, los casos son resueltos en los tribunales; se opera en el libre mercado, las sanciones no están tasadas, y **se incentiva la autorregulación[138].**

En cuanto al sector de la salud y más concretamente al historial clínico electrónico (EHR), en la UE las autoridades y organismos públicos han estado y están detrás del desarrollo y la implementación del EHR, mientras que en EE.UU. de nuevo el sector privado, especialmente compañías de seguros y organizaciones de salud, han liderado su desarrollo (George et al., 2012).

Miller y Tucker (2009) abordan el efecto de la regulación estatal de la privacidad en la difusión de registros médicos electrónicos, dada su capacidad para permitir a los proveedores de servicios de salud almacenar e intercambiar información de pacientes usando ordenadores en lugar de registros en papel; los hospitales pueden ser más propensos a adoptar EHRs si pueden garantizar a los pacientes que su confidencialidad está amparada por la ley. Por otra parte en cambio, la protección de la privacidad puede evitar el desarrollo de los EHRs y su adopción si los hospitales no pueden beneficiarse de un intercambio fácil y ágil de la información del paciente; la regulación de la privacidad a nivel estatal, que limita la capacidad de los hospitales para facilitar información de salud, reduce la adopción agregada de EHRs por los hospitales en más del 24%, según el estudio de Miller y Tucker.

Weiss y Archick (2016) recuerdan la posición de muchos funcionarios y representantes sectoriales de EE.UU. que mantienen la teoría de que un enfoque como el de EE.UU. (hacia la privacidad de los datos) es más ágil que el modelo europeo de "uno para todos".

Se trata pues de dos modelos claramente diferentes, uno donde la privacidad puede ser tratada como una mercancía que cada individuo, según su preferencia, puede vender o ceder a cambio de ciertos servicios, o si bien es un derecho básico del ser humano que debe ser protegido a toda costa (Voss, 2014; Shackelford, 2012; Steinke, 2002); mientras que la UE considera la intimidad como un derecho inalienable, EE.UU. parece tratar los datos de carácter personal más como una mercancía o un bien. La legislación europea tiene mayor cobertura para el individuo y es más restrictiva, utiliza el término “datos personales”, que comprende cualquier dato de una persona identificada o identificable, por lo que se deben tener en cuenta los datos de

138 La “autorresponsabilidad” como también se aborda la “autoregulación” es una buena respuesta y merece un impulso, pues se trata de mecanismos que buscan enfoques éticos que eviten riesgos cuando, en nombre de un objetivo económico, los derechos fundamentales de las personas pueden ponerse en peligro, aunque la autorregulación en sí misma no parece una respuesta suficientemente efectiva (Durán Cardo y García Morales, 2015).

empleados, proveedores, usuarios, clientes, etcétera; en EE.UU. la protección de datos hace referencia básicamente al consumidor y usuario (Johnson, 2007).

Merece la pena, en este contexto, hacer una breve mención a la República Popular China (en adelante, China) en cuanto al derecho a la protección de datos[139], o más bien su ausencia, pues representa un extremo muy alejado de la UE; en resumen, el modelo de la UE relativo a la protección de datos personales está muy lejos de China, que no ha promulgado una legislación que aborde específicamente la recolección, el almacenamiento y la transmisión, ni tampoco ha firmado ningún tratado con la UE ni ningún otro acuerdo similar como el que firmaron la UE y EE.UU. relativo al "Puerto Seguro" (ahora "Escudo de Privacidad"). No obstante, su Código Civil y su Ley de Responsabilidad Civil constituyen un recurso legal en caso de violación del derecho a la intimidad. Existen algunas disposiciones en las leyes y reglamentos en China que tienen relación con esta materia, pero por lo general se trata de protección de la información personal, que normalmente regula un sector específico (por ejemplo, el sector de las telecomunicaciones) o se refiere a cierta información de carácter específico. Aunque en la actualidad[140] no existe una definición específica de datos sensibles en la legislación china, pero se aplican normas especiales a ciertos tipos de datos de carácter personal, como son los registros médicos, la información sobre salud de la población, la información personal recopilada por los bancos comerciales, la información de crédito personal. Como recoge el Journal de la Cámara de Comercio de la UE en China[141], mientras existen muchas economías y regiones que ya han desarrollado legislaciones que proporcionan un marco estable para abordar estas cuestiones, **China sólo acaba de comenzar el proceso; la inmadurez de las leyes chinas y el carácter disperso de las normas aplicables a la protección de datos impiden un análisis adecuado del régimen de protección de datos del país.**

En EE.UU. el respeto a la privacidad está consagrado en su Constitución. Pero a diferencia de la UE no cuenta con un marco único de privacidad o protección de datos. Weiss y Archick (2016) sostienen que en general las leyes de privacidad de datos en EE.UU se entienden como un mosaico de normas federales y estatales; por una lado se aprobó en 1974 la Ley de Privacidad (*Privacy Act*), y en 1986 se promulgó la Ley de Privacidad de las Comunicaciones electrónicas, que amplió las restricciones gubernamentales para incluir las transmisiones de datos electrónicos, a la vez que existen una serie de leyes federales de protección del consumidor que son en gran medida específicas de cada sector, con diferentes normativas que rigen la recopilación y divulgación de datos financieros, datos relacionados con la salud, etcétera. La *Privacy Act* estableció normas para la protección de los datos en poder del Estado, y aunque han existido intentos por

[139] Data Protection in China. Recuperado de http://uk.practicallaw.com/4-519-9017. Último acceso el 12 diciembre de 2016.

[140] Información disponible a 1 de octubre de 2016.

[141] The present and future of data protection in China. Recuperado de http://www.eurobiz.com.cn/present-future-data-protection-china/. Último acceso 1 enero de 2017.

extender la protección al sector privado (Hoofnagle[142], 2006); a partir del 11 de septiembre (del año 2001) se impuso el principio de prevención del crimen, en el que se apoyan casi todos los programas del gobierno de EE.UU., que cambió su paradigma a un enfoque orientado a la prevención si cabe más allá de la resolución del delito.

Así, Craig y Ludloff (2011) señalan en su libro *"Privacy and Big Data"* que **existe un modelo de protección en EE.UU. de regulación netamente sectorial, donde no existe una única norma referida a la privacidad electrónica, y que está centrado especialmente en dos sectores (financiero y sanitario)** y en el ámbito de los menores de 13 años. La HIPAA[143] fue aprobada bajo el gobierno del Presidente Clinton, como norma sectorial para cubrir básicamente el sector sanitario. La regla de privacidad de la HIPAA es para autores como Rothstein (2016) notoriamente débil debido a su limitada cobertura, a las numerosas exclusiones y exenciones, y a los limitados derechos que asisten a los individuos. Los derechos del individuo son contemplados más bien como derechos de consumidor también en el ámbito de lo que respecta a su información sanitaria. Esta ley protege la cobertura de seguro médico a los trabajadores y sus familias cuando pierden su trabajo. Referida al ámbito de los menores[144], se exige a las páginas web que recogen información de niños menores de 13 años que tengan una política de privacidad explícita, define la responsabilidad de la página y las condiciones bajo las cuales se debe obtener consentimiento verificable del padre o de la madre. Por otro lado, las normas para la simplificación administrativa también regulan la seguridad y confidencialidad de los datos de salud; estas normas tienden a la mejora de la eficiencia y efectividad del sistema de salud, animando el uso generalizado del intercambio de datos electrónicos en el sistema de salud de EE.UU.

Aunque el modelo de regulación de la privacidad en EE.UU. se presenta complejo y segmentado, ello no debe llevar a la conclusión de que no se regula la privacidad o que se regula de forma muy superficial. La Comisión Federal de Comercio de los EE.UU. llegó a reunirse con representantes de Apple en 2014 para conocer todos los datos de salud que recoge HealthKit, y la forma en que conserva esa información[145]; como recogió la prensa la preocupación del organismo estadounidense parecía clara, y consistía en asegurar que los datos de salud (como datos sensibles) recopilados por sus dispositivos móviles y portátiles no se utilizarán ni comercializarán sin el consentimiento de los titulares, que ni Apple ni otras organizaciones puedan comercializar estos datos. Esta investigación tiene su razón de ser pues, según la Comisión Federal de Comercio, los desarrolladores de distintas aplicaciones móviles de salud y fitness han

[142] Chris Jay Hoofnagle es un profesor estadounidense en la Universidad de California, Berkeley, experto en privacidad de la información, y delitos informáticos. Recuperado de https://www.law.berkeley.edu/our-faculty/faculty-profiles/chris-hoofnagle/. Último acceso 3 enero 2017.

[143] Health Insurance Portability and Accountability Act de 1996.

[144] Según se recoge en la COPPA ("Children´s Online Privacy Protection Act").

[145] Los Angeles Times. FTC in talks with Apple about health data protection. Recuperado de http://www.latimes.com/business/technology/la-fi-tn-ftc-apple-health-privacy-20141114-story.html. Último acceso 10 de septiembre de 2016.

compartido información de sus usuarios con hasta 76 empresas, entre las que se encontraban varios anunciantes[146]; estos dispositivos guardan numerosos datos referidos a nuestros hábitos y comportamientos desde la mañana a la noche, y aunque pueden ser útiles para mejorar nuestra propia la calidad de vida, desde el punto de vista comercial son muy útiles, por lo que también se utilizan a menudo para venderlos a empresa de publicidad, compañías de seguros o farmacéuticas. La propia Comisión Federal de Comercio tiene en este sentido entre sus prioridades estudiar si los desarrolladores de aplicaciones móviles de salud en las plataformas iOS de Apple y Android de Google toman las precauciones necesarias para salvaguardar la privacidad de los usuarios de dichas aplicaciones. Pérez Morera (2016) estima que una de las mayores preocupaciones de las soluciones móviles orientadas al *eHealth* es la seguridad de los datos enviados, recibidos y almacenados, por lo que se hace necesario garantizar que las aplicaciones y sistemas desarrollados e implantados sean respetuosos con una serie de requisitos de seguridad, que define como **soluciones de seguridad** innovadoras para aplicaciones de *mHealth*.

La mayoría de los datos que los consumidores almacenan en aplicaciones de salud móviles no están cubiertos por las normas de privacidad norteamericanas conocidas como la anteriormente mencionada Ley de Portabilidad y Responsabilidad del Seguro de Salud, pero la Comisión Federal de Comercio de los EE.UU. ha destacado que estos datos continúan siendo altamente sensibles y es necesario por ello conocer cómo se comparten, intercambian y protegen los datos generados por los propios consumidores[147]; la agencia gubernamental norteamericana por lo tanto ha tomado cartas en el asunto y ha asumido como una prioridad la tarea de examinar, por ejemplo, si los desarrolladores de salud móvil de aplicaciones de marketing en el iOS de Apple y la plataforma Android de Google están tomando medidas para proteger la privacidad de los usuarios.

Sin embargo, al margen de estas consideraciones, es cierto que el modelo de EE.UU. deja la privacidad en manos del consumidor, para determinar el alcance de su protección e iniciar posibles demandas hacia una mayor regulación. Es más, bajo el sistema actualmente en vigor, existe una brecha entre la UE y los EE.UU., donde el régimen estadounidense otorga prioridad a la seguridad sobre la privacidad (Hatfield, 2016; Bender, 2014).

De hecho, como defiende Rothstein (2016), la *Privacy Rule* de HIPAA es notoriamente débil, por razón de su incompleta cobertura, numerosas exclusiones y exenciones, además de los limitados derechos para individuos.

[146] Reuters. U.S. FTC asking Apple about health data protection. Recuperado de http://www.reuters.com/article/us-apple-ftc-exclusive-idUSKCN0IX2I520141113. Último acceso 12 de septiembre de 2016.

[147] Reuters. U.S. FTC asking Apple about health data protection. Recuperado de http://www.reuters.com/article/us-apple-ftc-exclusive-idUSKCN0IX2I520141113. Último acceso 10 diciembre 2016.

En los EE.UU. los tribunales juegan un papel fundamental en la resolución de todo tipo de disputas, especialmente las relacionadas con bases de datos públicas (Freedom of Information Act) y relativas a la regulación de RAs (*consumer reporting agencies)* privadas; existen varias autoridades administrativas competentes para la aplicación de la ley (Fair Credit Reporting Act), entre las que se encuentran las autoridades de protección del consumidor y del sistema financiero, entre otras autoridades sectoriales. En la UE las leyes de protección de datos personales de Estados miembros se aplican, hasta la fecha, en primer lugar por parte de autoridades de control en cada país especializadas en protección de datos personales[148]; en general la protección de datos personales y el derecho de una persona a acceder a información sobre sí misma se refieren a derechos individuales. Los beneficios de una regulación de protección de datos (política de la UE) van más allá del individuo o consumidor cuyos datos se desean proteger. Todo esto puede haber conducido el 23 de septiembre de 2013 a que el US Department of Health and Human Services (HHS) refuerce la privacidad y la seguridad de la información sanitaria establecida en la HIPAA; los cambios mejoran considerablemente las protecciones de la privacidad del paciente, salvaguardando la información relativa a la salud del paciente en la creciente era digital; los pacientes tienen el derecho a solicitar que su proveedor de servicios de salud no informe o revele su información personal a las aseguradoras, a la hora de pagar los servicios médicos "completos": esta es una de las provisiones de la ley más comentadas respecto a los cambios en la HIPAA, la norma de privacidad de la salud que entró en vigor en 2013; el nuevo derecho parece útil pero la opción de pago "completo" conlleva una enorme complejidad[149], habrá pues que atender al **uso que hagan finalmente dichas aseguradoras de la información que puedan recabar.**

3.2.2. Uso de los datos personales.

Algunos principios tradicionales, al margen del juramento hipocrático y de la debida confidencialidad entre médico y paciente, han perdido su operatividad y efectividad en el contexto tecnológico actual, así los datos relativos a la salud presente o futura (previsible parcialmente gracias a la investigación genética) exigen una regulación específica que garantice los derechos de los individuos; algunas aseguradoras y centros de salud han sido sancionados en España por intercambiar información médica de los pacientes sin su consentimiento expreso (incumpliendo la normativa de protección de datos), sin embargo se les han aplicado sanciones reducidas por no apreciarse intencionalidad en la comisión de la infracción. La posibilidad de que las empresas en general (incluidas las aseguradoras) puedan obtener datos

[148] Del Villar R., de Leon A. D., & Hubert J. G. (2001). Regulation of Personal Data Protection and of Reporting Agencies: a Comparison of Selected Countries of Latin America, the United States and European Union Countries. *Credit Reporting Systems and the International Economy (MIT Press, Cambridge)*.

[149] The report "Paying out of Pocket to Protect Health Privacy: A New but Complicated HIPAA Option"; this is a report on the HIPAA Right to Restrict Disclosure that was published January 30, 2014, authors: Bob Gellman and Pam Dixon.

sin el consentimiento del interesado sigue levantado mucha controversia en Europa, y siendo motivo de algunas resoluciones de los organismos reguladores; Fernández Ruiz-Gálvez (2014) recuerda que las pruebas genéticas proporcionan información sobre salud actual (y futura) del paciente (y de sus familiares), lo que **supone un riesgo, también de discriminación, tanto a nivel laboral como en lo que respecta a los seguros de asistencia sanitaria y de vida**. El concepto de individuo con sus derechos fundamentales en Europa se distingue así con claridad del termino consumidor más empleado en EE.UU.; la evolución del modelo europeo ha acentuado las divergencias con el norteamericano (Martínez, 2014).

En 1995 se hizo por primera vez referencia a la protección de la personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos; se puede decir que este es el **primer hito hacia la normalización en la UE en materia de protección de datos**[150]. Sin embargo, antes de 1995 existían en Europa muy distintas leyes sobre privacidad; así el órgano de control del cumplimiento de la normativa de protección de datos en España, la Agencia Española de Protección de Datos (AEPD), fue creada en 1994[151].

De esta forma se desarrolla a partir de 1995 una normativa, en cada Estado miembro, adaptada a la Directiva. La norma española fundamental de referencia en esta materia[152] [153] se refiere expresamente a los datos de salud (considerándolos especialmente protegidos y limitando la posibilidad de su recopilación y cesión), aunque no define el concepto. Esta ley (LOPD) describe el dato personal como "cualquier información concerniente a personas físicas identificadas o identificables", asumiendo de este modo que cualquier dato que haya sido disociado o anonimizado debidamente no estará sujeto a la protección de la Ley.

El Comité de Ministros del Consejo de Europa en su Recomendación nº5, de 13 de febrero de 1997, referida a la protección de datos médicos, ya establecía que la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas; comprende, por tanto, toda información que permita formarse una idea de la situación médica de una persona, por ejemplo, a efectos de los seguros, como puede ser el comportamiento de una persona, su vida sexual, su

[150] Se trata de la Directiva Europea 95/46/CE de 24 de octubre del Parlamento Europeo y del Consejo.

[151] La AEPD se creó a partir de lo establecido en la derogada Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 29 de octubre de 1992 (LORTAD); ésta fue la primera Ley que reguló de forma específica esta materia en España.

[152] Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).

[153] Salom et al. (2002) realizan un análisis pormenorizado de la LOPD en su "Estudio sobre la Ley orgánica de protección de datos de carácter personal".

modo de vivir, su consumo de drogas, abuso del alcohol o del tabaco; serán considerados datos médicos, y estarán sujetos a una protección de nivel alto[154].

Sanz (2016) recoge que **la minería de datos, la codificación o la anonimización de los datos puede no siempre ofrecer la protección garantizada**: "en general, hasta ahora se consideraba que si los datos eran de dominio público, eran anónimos o estaban anonimizados, no era necesario requerir la aprobación de los interesados para su utilización. Sin embargo, la combinación de bases de datos puede llevar a identificar a personas singulares o a grupos que estaban de forma anónima en alguna de las colecciones de datos". Así, Sanz cita casos donde con fines de investigación se ha permitido la combinación de una base de datos anonimizada proporcionada por la *Group Insurance Commission* de Boston (donde no constaban los nombres, las direcciones, los números de la seguridad social, ni otro tipo de información identificativa), con otra base de datos, la de los votantes del Estado de Massachusetts en los EE.UU. (que incluía nombre, código postal, dirección, sexo, fecha de nacimiento) que sí es de dominio público; Sanz recoge cómo tras la combinación fue posible identificar a ciudadanos individualmente, y llegaron incluso a publicarse los datos médicos de la persona que ostentaba el cargo de gobernador de Massachusetts.

Existen iniciativas e **investigaciones que proceden del propio paciente**; el creciente acceso a la tecnología digital y el incremento de redes sociales digitales han facilitado la formación de comunidades en red donde los individuos implicados en investigación de temas sanitarios, abarcando la propia experimentación, la autovigilancia e interpretación de datos genómicos. Así, iniciativas como PatientsLikeMe[155] se presentan **con el potencial de generar un valioso conocimiento** sobre aspectos relacionados con la salud. Sin embargo, mientras algunos proyectos pueden ir acompañados de una colaboración con sistemas de investigación académica o empresarial, otros muchos no, y esto puede implicar **riesgos a todos los niveles para el rigor y validez de los mismos**[156]. Los ingresos de dicha compañía provienen de la colaboración, incluidas las compañías farmacéuticas, ya que la empresa vende datos anónimos del sitio web a estos socios o colaboradores. El objetivo general que se anuncia de estas asociaciones es aumentar las oportunidades de investigación, y así la empresa también colabora con instituciones académicas y asociaciones de pacientes.

[154] Artículo 4 del Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal aprobado por Real Decreto 994/1999 de 11 de junio.

[155] PatientsLikeMe Inc. fue fundada en 2004 y PatientsLikeMe.com abrió en marzo de 2006 para pacientes diagnosticados con ELA. El concepto de negocio deriva de la experiencia de tener un ser querido diagnosticado con ELA. Los fundadores están representados en el equipo directivo junto con varios inversores y fondos de capital riesgo. Estos inversionistas y fondos de capital riesgo tienen, en muchos casos, experiencia previa en la creación de negocios en la red que han logrado un gran éxito. Los pacientes con ciertos diagnósticos pueden convertirse en miembros sin cargo alguno. Los miembros de las diferentes comunidades de pacientes están diagnosticados con enfermedades como esclerosis lateral amiotrófica, sida, eslerosis multiple, epilepsia, parkinson y diversas formas de enfermedades mentales (www.patientslikeme.com).

[156] Tal y como recoge por el *Nuffield Council on Bioethics (febrero, 2015).* El almacenamiento, vinculación y uso de los datos en la investigación biomédica y la atención de la salud: cuestiones éticas.

Los propietarios de PatientsLikeMe describen que tienen una misión con este sitio web y es cambiar y democratizar el sistema de salud. Así, una de las condiciones de participación en el sitio es que los pacientes acepten esta visión. Los miembros del sitio web son invitados a participar en este cambio a través de su participación. **La generación de conocimiento a nivel social depende de la contribución de los miembros con su información y experiencia como pacientes**. Esto permite el intercambio de conocimientos a nivel de grupo, por ejemplo, en relación con PatientsLikeMe. Las redes sociales y la cooperación se destacan como dos de los elementos clave del concepto Medicina 2.0 (Eysenbach, 2008); el desarrollo de la Medicina 2.0 se erige **frente a los sistemas jerárquicos y cerrados** que tradicionalmente han caracterizado el ámbito del conocimiento de la salud.

Hay que recordar la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (llamada Directiva de ePrivacidad o ley de cookies), que fue diseñada para garantizar la seguridad de las comunicaciones, y que está ahora pendiente de revisión, para adaptarse al nuevo RGPD (cuya compleja reforma, que impone un gravoso régimen sancionar para los infractores, no ha facilitado su aprobación, aunque la normativa será efectiva desde el 25 mayo de 2018). En todo caso la reforma se hace necesaria de acuerdo con el Parlamento Europeo, aunque la Directiva ya había sido modificada en varias ocasiones. En marzo del año 2012 España incorporó dicha **Directiva comunitaria sobre privacidad electrónica**[157], y desde entonces todas las páginas web españolas que recopilan datos a través de cookies y tecnologías similares -siempre que estos archivos no sean estrictamente necesarios para el funcionamiento de la página- tienen obligación de informar con claridad sobre el tipo y la finalidad de los datos recolectados, además de obtener el consentimiento de los usuarios. En mayo del año 2013 la AEPD publicó con representantes del sector de la publicidad y los medios la "Guía sobre el uso de las cookies", destinada especialmente a editores web, con el fin de facilitar el cumplimiento de la nueva normativa. A la vista del protagonismo que en los últimos años han adquirido los crecientes medios de comunicación *online*, Ull (2015) ha estudiado el grado de transparencia y cumplimiento de la normativa en materia de privacidad y cookies por los principales medios *online* (también llamados cibermedios) generalistas de España; su investigación ha identificado las principales empresas en España que recolectan datos a través de cookies -empresas que, por su actividad, se denominan *Data Controllers*-; las conclusiones de su investigación señalan a ComScore, Google, DoubleClick (Google), Nielsen, Facebook, Cxense, Adsense (Google), Chartbeat, Digilant y WideOrbit como los principales *Data Controllers* que operan en España a través de cibermedios. Se trata de empresas (probablemente desconocidas para muchos usuarios) que disponen de técnicas de recopilación de datos por lo general poco transparentes e intrusivas; de aquí que aunque la ideología fundacional de Internet es la ideología de la libertad, la evolución de los últimos años podría llevar

[157] Real Decreto Ley 13/2012 de 30 de marzo.

a la "regresión", al convertirse en un **mecanismo de vigilancia como los definidos por Deleuze (2006) en sus "sociedades de control";** a pesar de todo, una vez más se constata que, junto a mecanismos de vigilancia, surgen herramientas que otorgan o facilitan la libertad y el protagonismo al individuo, sea en calidad de paciente, usuario, ciudadano o consumidor. Ello al tratarse especialmente de herramientas con un mayor anonimato (al menos teóricamente), que permiten al internauta internarse en el ciberespacio.

3.2.3. Prevención versus tratamiento.

El gasto en salud en los países de la OCDE representó de media el 9.3% del PIB en 2012, frente al 9.2% en 2011, aunque con recortes significativos en países como España, Grecia, Italia, Portugal, República Checa y Hungría[158]. En EE.UU. el gasto en salud representó en 2012 el 17.2% del PIB[159], y creció por encima de la media de la OCDE pero similar a las tasas de crecimiento en 2010 y 2011. En la literatura científica más reciente se abarcan los retos que afectan al ámbito de la sanidad digital tanto en la UE, EE.UU. como en otros países de la OCDE, desde el punto de vista de las leyes, la ética y la gobernanza; se trata de impulsar la sanidad electrónica como un nuevo modelo basado en la prevención, más que en los síntomas de las enfermedades, y en la persona, más que en el tratamiento médico en hospitales; así lo entienden George et al. (2013), que realizan importantes contribuciones sobre la sanidad electrónica, aportando soluciones y alguna recomendación referidas a **las buenas prácticas.**

Dos metas se persiguen con este modelo: (1) la mejora de la calidad de vida y (2) la reducción de costes sanitarios. La informatización ha sido identificada como un medio para reducir los costes de la sanidad; Bates (1997) trata de los crecientes costes de los servicios de salud; aunque los datos médicos informáticos se usan especialmente en hospitales y clínicas, queda patente que esos datos se usarán en cada vez más numerosos y diversos entornos. Los sistemas informáticos interconectados permiten compartir información, como por ejemplo, una radiografía tomada unos años antes en otro lugar. Sin embargo, estos sistemas presentan serios riesgos para la privacidad. Según se recortan ciertos costes y servicios médicos, hay que medir la calidad de forma rutinaria, para saber cuando la privacidad puede verse afectada. Las bases de datos compartidas por distintas organizaciones son muy útiles pues permiten identificar problemas que de otro modo se pasarían por alto. Pero por otro lado, aunque los controles de privacidad son siempre importantes, se hacen todavía más necesarios ante el crecimiento de incentivos financieros a la investigación, con fines comerciales. Bates aborda los riesgos de la creciente informatización para la confidencialidad, a medida que las organizaciones y ciertas empresas del sector sanitario se plantean

[158] Según datos de la Organisation for Economic Co-operation and Development (OECD, en español OCDE).

[159] Martin, Hartman, Whittle, Catlin, y National Health Expenditure Accounts Team (2014).

gestionar información específica relativa a los pacientes en Internet, el riesgo va en aumento. La sociedad actual tendrá que elegir entre la privacidad o la eficacia en la prestación de servicios de salud al paciente, como insiste Bates.

La Comisión Europea ha revelado un plan de acción para eliminar las barreras que impiden el pleno uso de soluciones digitales en los sistemas de salud europeos. La meta final es mejorar la atención sanitaria para el beneficio de los pacientes, dar a los pacientes mayor control sobre dicha atención a la vez que se reducen los costes. Mientras pacientes y profesionales recurren cada vez más a soluciones de telemedicina y muchos europeos se bajan aplicaciones móviles para el seguimiento de su propia salud y su bienestar, más allá del potencial, todavía queda lograr una efectiva mejora de la salud junto con una reducción de costes (Williams, 2010).

El plan de acción de la UE[160] pretende incrementar el ritmo de transformación y mejora de la atención sanitaria mediante las siguientes medidas:
-aclarando áreas de inseguridad jurídica;
-mejorando interoperabilidad entre sistemas;
-aumentando la sensibilización y las habilidades entre pacientes y profesionales de la salud;
-situando a los pacientes en el lugar protagonista con iniciativas relacionadas con la propia gestión de la salud y apoyando la investigación tendente a la medicina personalizada;
-asegurando asesoramiento legal gratuito para iniciativas emprendedoras en materia de *eHealth.*

Además, la Comisión emitió un "*mHealth (Mobile Health) Green Paper*" en 2014 abordando aspectos de calidad y transparencia, aunque la Comisión Europea se ha implicado en materia de *eHealth* desde 2004[161]. Para preparar un nuevo plan, la Comisión realizó una consulta pública entre el 31 de marzo de 2011 y el 30 de mayo de 2011, determinando que la privacidad y la protección de datos eran áreas donde había que centrarse (y que sirvió de base para la definición del *eHealth Action Plan 2012-2020)*[162]. De hecho, **la falta de mayores mecanismos de control gubernamental ha supuesto por mucho tiempo una barrera para obtener la confianza de los ciudadanos/pacientes para el desarrollo de la HCE**; Terry y Francis (2007).

En este sentido, el análisis de la creciente variedad de tipos de aplicaciones móviles de salud conduce a la necesidad de resaltar una cuestión relevante de cara a los usuarios de las mismas, que consiste en saber qué tipo de seguridad implementar a cada uno de los tipos de aplicaciones, de acuerdo con sus

[160] MEMO/12/959 de la Comisión Europea, del 7 de diciembre de 2012.

[161] European Environment & Health Action Plan 2004-2010.

[162] Que a su vez responde a la petición de 2009 de los Estados miembros.

características; se trata de **preservar la privacidad pero también la seguridad** en aplicaciones móviles de esta índole pues tratan información especialmente sensible de los usuarios (Pérez Morera, 2016).

Por todo ello, como señalan Luxton, Kayl y Mishkind (2012) **la ausencia de una normalización en la seguridad de los datos supone una barrera para garantizar la privacidad, y permitir la interoperabilidad de sistemas**, para maximizar las capacidades de los dispositivos móviles, en detrimento del avance de iniciativas de *eHealth*.

Ya en 2008 se emitió la primera Recomendación sobre HCEs interoperativas. **Para que estas HCEs sean interoperativas es necesaria la normalización de los mismos, lo que hará posible la interconectividad electrónica entre sistemas de salud**. Se trata de lograr la interoperabilidad de acceso, pero para ello es necesaria la previa unificación semántica, es decir que el lenguaje o terminología sanitarios estén normalizados. Así lo indica Knoppers (2005), quién además de la gobernanza y seguridad, estima que es necesario un lenguaje similar, codificado o anonimizado, que anime y fomente a la colaboración internacional; más aún, las barreras actuales que dificultan la creación de biobancos de población y las herramientas de fomento de la protección de datos y su acceso, deben analizarse desde una perspectiva más amplia referida al genoma, la seguridad de los datos y la ética, para no desincentivar la participación de posibles interesados. Sin embargo, existe una tendencia internacional, que no se puede ignorar, relativa al creciente número de biobancos alrededor del mundo, desde EE.UU. (donde hay al menos 30 instituciones implicadas), a China, pasando por el Reino Unido (Rothstein y Knoppers, 2016).

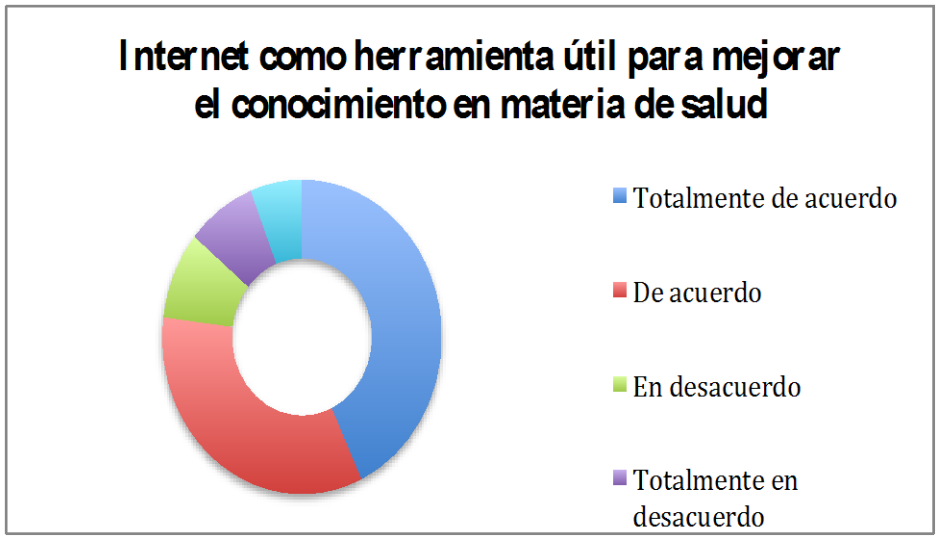
A principios de 2012 la UE aprobó el Proyecto de Reglamento europeo de protección de datos en sustitución de la actual Directiva 95/46/CE, precisamente para hacer frente a estos cambios; la normativa del nuevo RGPD se aplicará desde el 25 de mayo de 2015 de forma general en todos los Estados miembros, y con ella todos los Estados miembros estarán sujetos al **nuevo escenario de seguridad y protección de datos**.

3.3. Actitudes de los ciudadanos europeos.

En este apartado se trata sobre la protección de datos e identidad electrónica de los ciudadanos europeos en función de su país de origen, y se pretende con ello constatar la tendencia a la armonización liderada por los propios europeos.

De acuerdo con la encuesta de la un 59% de los ciudadanos europeos utilizaron Internet como fuente de información sobre salud en los doce meses anteriores al estudio[163].

Figura 3.2.
Internet como herramienta para buscar información de salud.



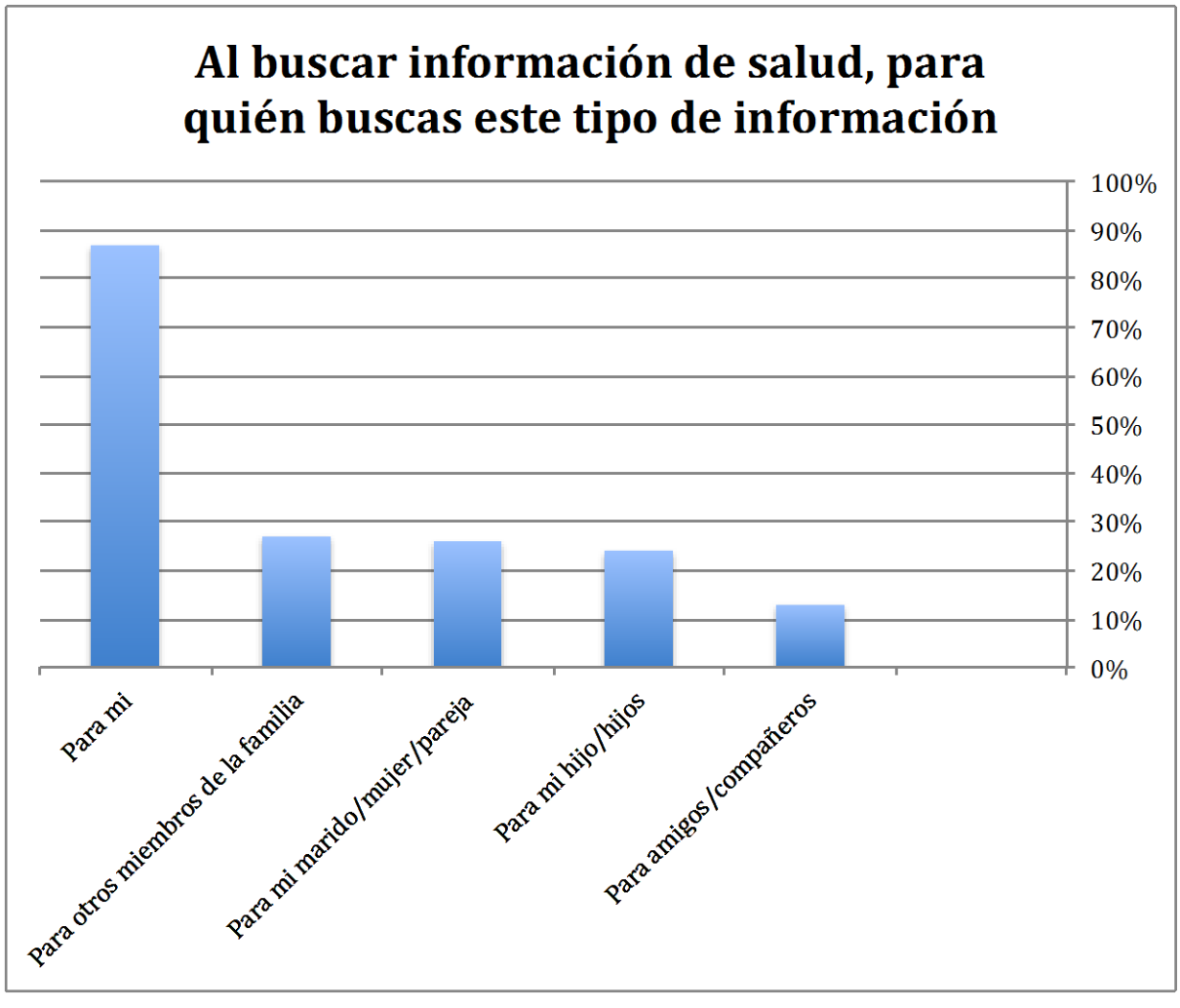
Fuente: figura del Flash Eurobarometer 404

Del estudio y los porcentajes reflejados en la figura 3.2. se desprende que Internet es una buena herramienta (de acuerdo con un 77% de los ciudadanos comunitarios encuestados) para mejorar sus conocimientos sobre salud, frente a sólo un 17%. En general el estudio revela que un 83% valora los contenidos *online* como suficientes, fiables y comprensibles, mientras que un 25% de los encuestados se siente más confundido al acudir a la red para obtener información de índole sanitaria.

El gráfico 3.0. más abajo confirma que **la gran mayoría de ciudadanos europeos que han buscado información sobre salud en Internet lo han hecho para sí mismos**, bien sea información general (87%), información relativa a una lesión o estado de salud (78%), o una segunda opinión (78%), o información referente a un tratamiento o proceder médico (76%). Proporciones parecidas se reproducen cuando los encuestados buscan información para otros miembros de su familia (entre 27% y un 30%, dependiendo del tipo de información buscada), para su marido/mujer o pareja (entre un 23% y un 26%) o para sus hijos (entre un 22 y un 26%). Sólo una minoría buscan información para un amigo o compañero (entre un 8% y un 13%, dependiendo de la información que se busque).

[163] principalmente para asuntos relativos a estilos de vida saludables y bienestar psicológico.

Gráfico 3.0.
Para quién buscamos información de salud en Internet.



Fuente: gráfico de elaboración propia a partir de datos del Flash Eurobarometer 404

Este estudio confirma la tesis de Bylund et al. (2012) quienes señalan por qué Internet juega un papel relevante en lo que se refiere a situaciones cómo las que viven los pacientes afectados de cáncer, cómo entienden su enfermedad, el diagnóstico y el tratamiento.

Asimismo, este estudio señala las **fuentes líderes de información sobre salud en Internet**: (1º) entre el 82% y el 87% (dependiendo del tipo de información buscada) de los que buscaron información sobre la salud lo hicieron a través de motores de búsqueda, (2º) entre el 47% y el 48% lo hicieron a través de páginas web especializadas (blogs y foros), (3º) entre un 33% y un 38% buscaron información en páginas web oficiales (ministerios de salud, organización mundial de la salud, etcétera), seguido de (4º) periódicos o revistas digitales (20-26%), (5º) redes sociales (con un 16% a un 23%), (6º) aplicaciones de salud para móviles (13% a un 17%) y páginas web de organizaciones de pacientes (con el mismo porcentaje).

Una gran mayoría de los europeos entrevistados[164] (74%) consideran la información médica, datos de pacientes e información de salud, como algo personal, especialmente en países del norte y oeste de la UE (tabla 3.0.), aunque sólo un tercio (33%) de los europeos son conscientes de la existencia de una autoridad pública nacional que es responsable de proteger sus derechos.

[164] Datos procedentes del Eurobarómetro especial 359 sobre "actitudes sobre protección de datos e identidad electrónica en la Unión Europea", publicado en Junio de 2011.

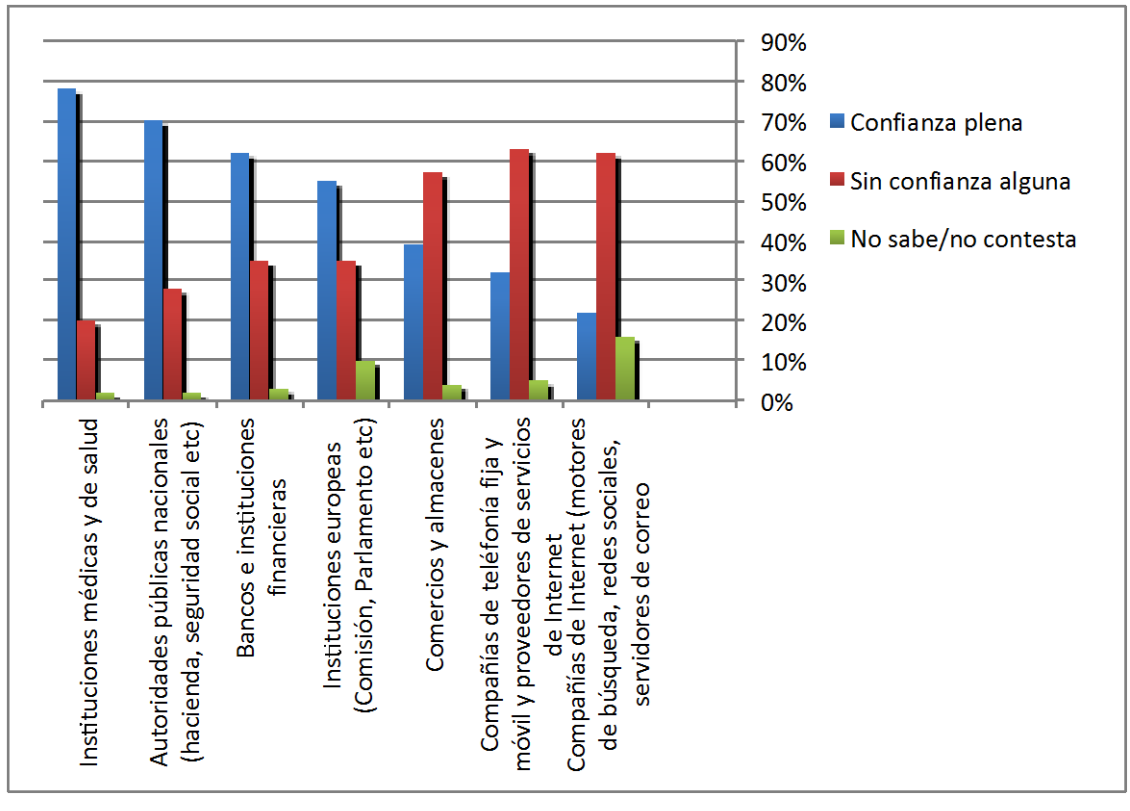
Tabla 3.0.
Actitudes de los ciudadanos europeos.

	Consideran la información médica (datos de salud) como algo personal	Tienen confianza plena en las instituciones médicas y de salud que recogen y almacenan datos personales	Tienen confianza plena en compañías de Internet; motores de búsqueda, redes sociales, proveedores de correo electrónico	Consideran importante tener los mismos derechos y protecciones sobre la información personal con independencia del país de la UE en que se recojan y traten los datos.
Media de la UE de los 27	**74%**	**78%**	**22%**	**90%**
Irlanda	93%	80%	29%	94%
Eslovenia	90%	82%	22%	94%
Suecia	89%	88%	26%	93%
Dinamarca	87%	93%	32%	91%
Alemania	87%	79%	16%	89%
República Checa	87%	79%	25%	91%
Holanda	86%	83%	20%	92%
Luxemburgo	85%	90%	17%	90%
Bélgica	84%	91%	23%	92%
Eslovaquia	84%	84%	32%	94%
Reino Unido	83%	83%	30%	95%
Francia	82%	86%	16%	93%
Estonia	81%	87%	32%	86%
Finlandia	80%	90%	33%	95%
Malta	79%	89%	20%	93%
Letonia	77%	70%	28%	82%
Austria	75%	79%	21%	89%
Italia	67%	68%	23%	87%
Lituania	66%	71%	28%	84%
España	65%	85%	18%	88%
Chipre	64%	78%	12%	95%
Grecia	62%	58%	14%	95%
Hungría	61%	83%	24%	91%
Bulgaria	52%	73%	20%	86%
Rumania	50%	61%	22%	79%
Portugal	50%	79%	25%	86%
Polonia	48%	63%	26%	90%

Fuente: Tabla de elaboración propia a partir de datos del Eurobarómetro especial 359 de la Comisión Europea sobre "actitudes sobre protección de datos e identidad electrónica en la Unión Europea".

Los europeos en un elevado porcentaje (78%) tienen confianza plena en las instituciones médicas y sanitarias, por encima de las instituciones europeas (un 55%), como refleja el gráfico 3.1; aunque una minoría (sólo un 22%) confía en los motores de búsqueda y las redes sociales, algo que debe hacer reflexionar; en esta línea, la confianza de los europeos en comercios y almacenes en general (un 39%) y en compañías de telefonía fija y móvil así como en proveedores de Internet (32%), revela que existe una mayor confianza en autoridades e instituciones en general que en compañías y en Internet, lo cuál es un indicativo de la viabilidad de una armonización liderada por las instituciones europeas (9).

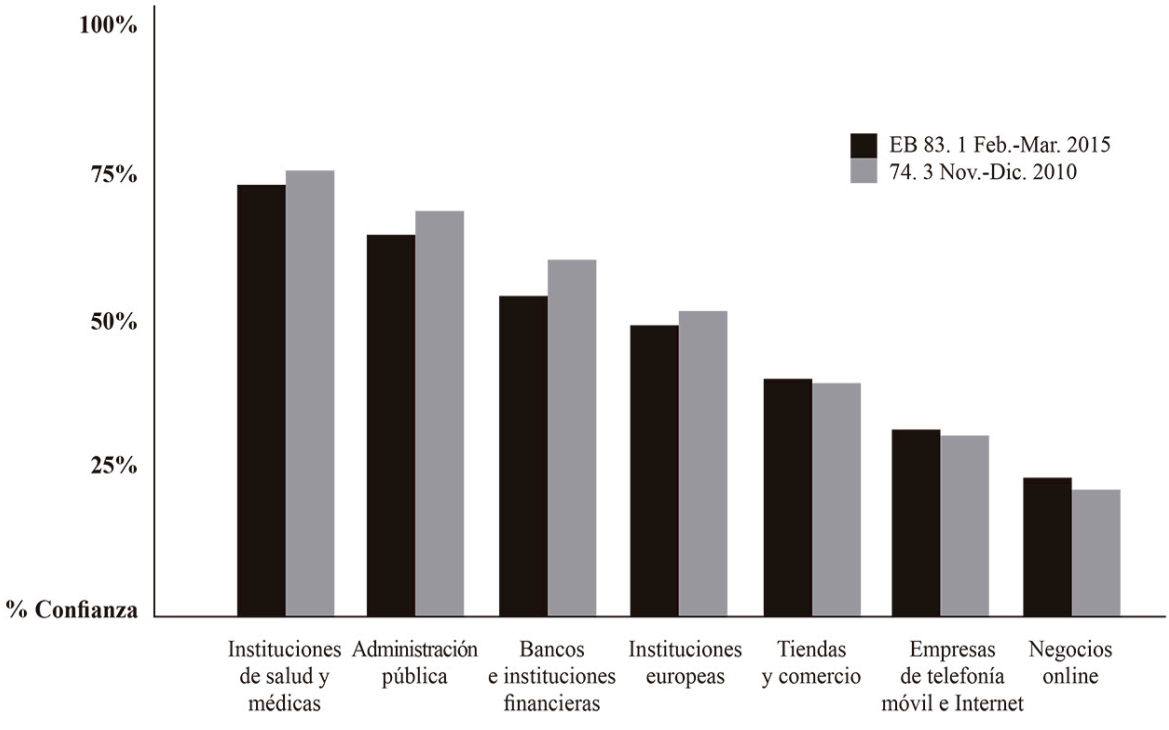
Gráfico 3.1.
Confianza de los ciudadanos europeos en sus instituciones y empresas que recogen y almacenan datos.



Fuente: gráfico de elaboración propia a partir de datos del Eurobarómetro especial 359 de la Comisión Europea sobre "actitudes sobre protección de datos e identidad electrónica en la Unión Europea".

En el siguiente gráfico 3.2. se puede comparar la evolución desde 2011 a 2015, para comprobar la escasa variación casi 5 años más tarde, cuando sólo un 24% confía en empresas de Internet (incluyendo aquí redes sociales y servicios de correo electrónico), y sólo 33% confía en proveedores de servicios de Internet.

Gráfico 3.2.
Evolución de la confianza de los ciudadanos europeos en autoridades y empresas que recogen y almacenan datos.



Fuente: elaboración propia a partir de datos el Eurobarómetro especial 431

Los usuarios más jóvenes en la UE, de 15 a 24 años, nacidos en la era digital, y estudiantes, son más proclives a la revelación de datos personales, aspecto sin mayor trascendencia para ellos (tabla 3.1.); no tienen problema en facilitar datos personales a cambio de servicios gratuitos en Internet, tales como una cuenta de correo gratuita, y sienten la necesidad de revelar información personal en Internet; es probable que faciliten distintos datos personales en redes sociales, y que no lleguen a leer las políticas de privacidad (y por ende los contratos) que rigen, que se sientan suficientemente informados sobre la recogida de datos y consiguientes usos de sus datos cuando se dan de alta en una red social o se registran en un servicio electrónico. Estos usuarios confían en todas las autoridades, instituciones y compañías, como responsables del correcto tratamiento de sus datos. Es poco probable que estos usuarios vean un riesgo en el uso de su información, en la posible infracción de las políticas de privacidad, en el tratamiento que las empresas electrónicas puedan hacer de sus datos.

A pesar de ello, hay que recordar lo que apuntan autores como Bonneau y Preibusch (2010), cuando se refieren a que existen muchos malentendidos sobre las razones de las infracciones a la privacidad, aludiendo a la opinión extendida de que ocurren frecuentemente porque la generación de usuarios de las redes sociales, gente joven especialmente familiarizada con las nuevas tecnologías, no se preocupan de la privacidad.

Frente a los usuarios más jóvenes, hay otros familiarizados con Internet a través de su trabajo o de su formación, más que por razón de su edad; son profesionales que tienen responsabilidades directivas. En contraste con los más jóvenes, son conscientes de los riesgos y se preocupan por el uso que se pueda dar a sus datos. A mayor nivel de formación, mayor concienciación sobre la privacidad. Es improbable que sientan que tienen el control de sus datos en Internet, o la posibilidad de eliminarlos cuando lo deseen, tanto en compras en Internet como en el uso de las redes sociales. A la vez, como dato curioso, es más probable que estén dispuestos a pagar por el acceso a información personal que pueda estar a disposición de compañías públicas o privadas.

Tabla 3.1.
Valoración de los datos personales de los europeos por razón de sexo, edad, estudios, profesión, uso de Internet, capacidad adquisitiva y escala social.

	Consideran la información médica como dato personal	Consideran que para obtener productos/servicios hay que facilitar datos personales	Preocupados a la hora de facilitar datos personales
Sexo			
Hombres	72%	60%	60%
Mujeres	75%	57%	64%
Edad			
15-24	71%	69%	55%
25-39	75%	66%	63%
40-54	76%	59%	66%
55 o más	72%	47%	62%
Estudios (finalización)			
15-	67%	47%	60%
16-18	74%	59%	63%
20+	81%	63%	67%
Todavía estudiando	71%	67%	56%
Actividad profesional			
Por cuenta propia	74%	61%	65%
Directivos	83%	66%	71%
Otros profesionales	78%	65%	62%
Operarios/obreros	75%	62%	63%
Servicio doméstico	68%	58%	65%
Desempleados	70%	59%	60%
Jubilados	71%	46%	60%
Estudiantes	71%	67%	56%
Uso de Internet			
Todos los días	80%	67%	64%
Con frecuencia/a veces	74%	62%	66%
Nunca	68%	45%	60%
Con dificultades para pagar facturas			
La mayor parte del tiempo	69%	N/A	N/A
De vez en cuando	70%	N/A	N/A
Casi nunca	76%	N/A	N/A
Según se incluyan en la escala social			
Baja (1-4)	70%	N/A	N/A
Media (5-6)	74%	N/A	N/A
Alta (7-10)	76%	N/A	N/A

Fuente: datos del Eurobarómetro especial 359 de la Comisión Europea sobre “actitudes sobre protección de datos e identidad electrónica en la Unión Europea”.

Atendiendo a las 5 principales economías europeas, el 65% de los españoles considera necesaria la autorización de los padres para la cesión de datos de menores (de 18 años) en Internet165 (tabla 3.2.); la mayoría de los padres encuestados ven necesario dar su permiso si una empresa solicita datos personales a sus hijos. Los británicos ven necesario ese consentimiento paterno en un 35% de los casos, los alemanes en un 57%, los españoles en un 65%, los franceses en un 52% y los italianos en un 59%. A pesar de la Directiva europea, la edad en la que se requiere el consentimiento paterno para la recogida y tratamiento de los datos varía de un país a otro.

Tabla 3.2.
Autorización paterna en Europa para la cesión de datos y capacidad legal de los menores.

	Consideran necesaria la autorización paterna para la cesión de datos de menores en Internet	Capacidad legal de los menores para prestar su consentimiento al tratamiento de sus datos
España	65%	Los menores tienen capacidad a los 14 años, pero para edades inferiores es necesario el consentimiento de los padres o tutores legales
Francia	52%	Los únicos datos que pueden dar los menores en la subscripción a newsletters son el e-mail y la edad.
Alemania	57%	Los padres han de dar su consentimiento antes de los 14 años, entre los 14-16 años sólo han de darlo dependiendo de qué tema se trate y capacidad de comprensión.
Italia	59%	Los menores de 18 años no pueden dar su consentimiento para la consecución de bienes y servicios.
Reino Unido	35%	Se requiere consentimiento paterno para menores de 13 años.

Fuente: datos del Eurobarómetro especial 359 de la Comisión Europea sobre "actitudes sobre protección de datos e identidad electrónica en la Unión Europea".

Se puede concluir que la mayor parte de los europeos han aceptado que el uso de datos de carácter personal es un hecho en la vida moderna, a la vez que muestran preocupación por la confidencialidad. Informar a los ciudadanos europeos sobre las implicaciones derivadas del uso de datos de carácter personal puede ayudar a una mayor concienciación sobre su trascendencia, a la vez que puede animarles a ser más prudentes a la hora de revelar esos datos de carácter personal. **Prácticamente todos los europeos (90%) están a favor de una armonización de los derechos a la protección de la privacidad en la UE**, y una mayoría (44%) preferiría que la normativa y sus sanciones se hicieran efectivas desde órganos de control a nivel paneuropeo, en lugar de a nivel nacional (40%) o regional (10%).

[165] Según el estudio titulado «La fiebre del oro de los datos» realizado por el bufete Osborne Clarke en 2012 en el que analiza y compara el comportamiento de los ciudadanos de España, Reino Unido, Alemania, Francia e Italia a la hora de facilitar información personal tanto en páginas web como en motores de búsqueda.

3.4. Adaptación a un marco legal unificado, en un contexto con sistemas sanitarios y entornos culturales diversos.

En este apartado se identifican los desafíos existentes, técnicos, lingüísticos, incluidos los entornos culturales, de cara al desarrollo de sistemas integrados de protección en el entorno *eHealth* a nivel internacional.

3.4.1. Recomendaciones en el entorno del Big Data y *eHealth*.

Desde el punto de vista jurídico es cierto que existe complejidad en el ordenamiento jurídico dentro de Europa, pero se trata de un sistema integral, de reconocimiento y tutela de derechos fundamentales, en evolución; como señalaba Sanjuan (2005) este sistema se alimenta de varias fuentes, a saber: (1) la europea comunitaria (2) la derivada del Convenio Europeo de Derechos Humanos y (3) el derecho interno, pero está más armonizado de lo que se puede pensar de forma generalizada, y representa los pilares sobre los que se asienta el patrimonio europeo común.

Como señalan Bates y Wright (2009), a pesar de las numerosas oportunidades que existen para la colaboración transnacional, hay que superar barreras importantes como la lingüística; unos 261 idiomas son hablados en el mundo por más de 1 millón de personas como lengua materna, y muchas de estos idiomas disponen de distintos alfabetos. Este elevado número de idiomas representa un desafío enorme a la hora de traducir algunas aplicaciones de *eHealth*. En países en desarrollo, la mayor parte de la actividad de *eHealth* se dirige a profesionales sanitarios, que suelen dominar una lengua vehicular internacional (frecuentemente el inglés). La traducción de aplicaciones de *eHealth* a lenguas locales también suscita el interrogante del nivel de alfabetización y los conocimientos informáticos, algo que varía según qué proveedores de servicios sanitarios, y especialmente entre los propios pacientes. Para estos investigadores las diferencias culturales y sociales son barreras más difíciles de superar. Por otro lado, surgen grandes diferencias entre (y dentro de) los países respecto a exigencias éticas y gobernanza de las investigaciones; como han identificado Elwyn, Seagrove, Thorne y Cheung (2005) estas diferencias incrementaron en 150 días en el estudio de una multinacional, y de acuerdo con la investigación de Hearnshaw (2004) la comparativa entre países europeos también identificó variaciones sustanciales. Existen muchos otros desafíos derivados de los distintos sistemas sanitarios, de sus estructuras, de su actividad. El análisis financiero de los sistemas resulta aún más complejo por sus diferentes políticas de reembolsos, por ejemplo. Otra barrera identificada es la financiación de la investigación en salud digital, que suele provenir de las arcas de cada país, y no de fuentes internacionales, con la excepción de la UE.

Las barreras potenciales para compartir datos en sistemas de salud pública son variadas: técnicas, motivacionales, económicas, políticas, legales y éticas; Van Panhuis et al. (2014). La UE es considera hoy como la jurisdicción más regulada a nivel mundial en materia de protección de datos y privacidad. Conviene analizar la situación en Europa sobre cultura de protección de datos para entender por qué. En este contexto hay que señalar se considera que sólo el interés público puede ser una excepción para obtener y transmitir información médica del paciente (contenida en la HCE) sin su consentimiento, y el paciente siempre puede oponer su derecho a compartir la información (frente a la limitación de este derecho en EE.UU.). La presunción de protección de la privacidad en la UE puede servir para ganarse la confianza de los usuarios, (frente a los EE.UU. donde no existe presunción de privacidad, lo que puede provocar el efecto contrario en los pacientes). En general, la normativa de la UE ha avanzado más hacia el doble objetivo de una eficiente implementación de la HCE y la protección de la privacidad gracias al control que ejerce el paciente. Así "la falta de mecanismos de protección gubernamental...puede que no inspire la confianza del paciente/ciudadano en la HCE. Queda patente que la seguridad de la información sobre la salud del paciente resulta exponencialmente más importante en un sistema que permite compartir esa información electrónicamente de manera generalizada" (Hiller, McMullen, Chumney y Baumer, 2011); parece que los Estados miembros de la UE se acercan al modelo ideal adoptando la HCE a la vez que reafirman su compromiso con los principios de protección de la privacidad de los pacientes; si se pretende que la HCE en EE.UU. tenga un uso generalizado y ofrezca verdaderos beneficios, los aspectos de privacidad y seguridad de la información sanitaria de cada paciente deben jugar un papel central en los trabajos de implementación.

En cuanto a la magnitud de los avances en materia de protección de datos sensibles, los datos de salud, la medicina está exprimiendo la tecnología a gran velocidad, con importantes **implicaciones éticas, legales y sociales** derivadas de compartir cada vez un mayor número de datos potencialmente sensibles, que podrían obstaculizar o impedir su uso si no tratan de forma adecuada (Dyke, Dove y Knoppers, 2016). Por ello, la normativa de la UE avanza hacia ese doble objetivo de una eficiente implementación de la HCE y la efectiva protección de la privacidad, donde **el individuo ejerce el control**; un sistema enfocado al individuo y no tanto al mero consumidor; por ello, la concienciación desempeña un papel central pues sin ella los individuos no podrán ejercer sus derechos ante las autoridades competentes o ante los tribunales.

El estudio de la Comisión Europea (sobre Big Data en salud pública, telemedicina y atención sanitaria)[166], elaborado en el desarrollo del tercer Programa de Salud de la UE (2014-2020) bajo el mandato de la Comisión Europea, ha propuesto una serie de recomendaciones relativas a la sensibilización, educación y formación, fuentes de datos, intercambio abierto de datos e intercambio de datos, aplicaciones y propósitos, análisis de datos, gobernanza del acceso y uso de los datos, financiación y recursos financieros, así somo los aspectos legales y la regulación de la privacidad; estas diez recomendaciones (ver figura 3.1.)

[166] Comisión Europea. "*Study on Big Data in Public Health, Telemedicine and Healthcare*", 16 diciembre 2016.

ofrecen una clara orientación a los responsables de la toma de decisiones y a los propios ciudadanos de la UE respecto a la mejor manera de utilizar el Big Data en materia de salud. Aquí paso a abordar cada una de ellas en detalle:

3.4.1.1. Sensibilización.

En la preparación de cada estrategia de comunicación por Estado miembros se recomienda involucrar a todas las partes interesadas pertinentes, muy especialmente a los representantes de los pacientes, para garantizar un amplio compromiso del público e interesados en general. La Comisión Europea puede contribuir al desarrollo de cada proceso en los Estados miembros facilitando ejemplos de buenas prácticas y herramientas. El objetivo consiste en provocar un diálogo continuo y abierto con todas las partes interesadas y grupos de pacientes, que podría fomentarse, por ejemplo, mediante la creación de una plataforma europea de intercambio de experiencias.

El modelo europeo pretende alentar una mentalidad positiva de la opinión pública hacia el Big Data en materia de salud, a través de un diálogo entre todas las partes interesadas, y de información basada en hechos. Se aboga por que todos los interesados (pacientes, proveedores de atención sanitaria, vendedores de tecnología, etcétera) asuman como propio el objetivo de reducir las reticencias, muchas veces injustificadas, hacia el uso del Big Data en *Health.* Sensibilizar sobre el uso práctico del Big Data en el área de la salud y sus beneficios debe tener un papel relevante, para que sea tangible y comprensible.

Se trata de desarrollar e implantar una estrategia de comunicación para que crezca la concienciación sobre el valor añadido del Big Data en materia de salud, y promover una mentalidad pública positiva hacia el uso del Big Data en materia de salud. La Comisión Europea quiere fomentar el desarrollo de una estrategia que comunique de forma consistente el valor añadido (y científicamente probado como afirma el informe) del Big Data en materia de salud en general y de salud pública en particular, a la vez que se ocupa de las prevenciones relativas a la protección de datos y el posible uso indebido de los datos recolectados. Se propone en consecuencia (1) un alineamiento de todos los esfuerzos a nivel nacional y comunitario en materia de comunicación y sensibilización (2) crear evidencias científicas del valor agregado del Big Data en el campo de la salud, y (3) consolidar el concepto de que el Big Data en *eHealth* permite aprovechar y generar un conocimiento valioso, para lograr una mayor calidad y eficiencia en la atención sanitaria de los ciudadanos europeos, a través de **buenas prácticas** (ver apartado 3.4.4.).

El plan de comunicación debe contar con todas las partes interesadas, e informarles sobre los ventajas y beneficios concretos que se pueden obtener, así como los riesgos a evitar al recurrir al Big Data en salud. Se considera clave en el desarrollo de la estrategia que vaya acompañada de la participación de las

organizaciones de pacientes para ganarse la confianza de los pacientes en la aplicación del Big Data en salud. Los profesionales de la salud, y los responsables de la toma de decisiones en la política de salud y la propia industria tienen involucrarse para identificar cuestiones relevantes para sus intereses y para averiguar si, y en qué medida, la aplicación del Big Data puede aportar soluciones. Es conveniente identificar los grupos objetivo para la estrategia, dentro de los principales grupos de interés (como, por ejemplo, personas con perfil menos técnico). La estrategia debe garantizar que la comunicación llega a ciudadanos y pacientes, teniendo en cuenta las circunstancias específicas de cada país.

3.4.1.2. Educación y formación.

Existe la creciente necesidad de una fuerza de trabajo que pueda utilizar el potencial del Big Data en *eHealth*, por lo que se trata de fortalecer el capital humano. A través de la información y la educación debe propiciarse la **alfabetización digital en materia de salud de los profesionales sanitarios y de los profesionales de la salud en general**.

La Comisión Europea promueve el intercambio de conocimientos sobre el Big Data en el área de la salud, incluida la integración de la gestión de datos en los planes de estudio de los profesionales de la salud, financiando las iniciativas que sean pertinentes con este fin. La adaptación y la mejora del sistema educativo para fortalecer el capital humano del Big Data en salud debe desarrollarse a nivel nacional pero la cooperación a nivel de la UE puede contribuir a su éxito.

El creciente número de fuentes disponibles, accesibles y utilizables de Big Data, conduce a una creciente demanda de capital humano. Los programas de educación y formación existentes para la salud pública o la salud deben integrar en los planes de estudio la gestión de los datos en los planes de estudio para asegurar el desarrollo de las destrezas y competencias necesarias. Si bien en algunas regiones las nuevas áreas de trabajo, como la referida a los analistas de datos de salud, ya están evolucionando, se recomienda aumentar los recursos de **capacitación en el campo de la gestión de datos y sistemas**, el análisis estadístico avanzado y las tecnologías de la información para los científicos que trabajan con Big Data.

3.4.1.3. Fuentes de datos.

La ampliación de las fuentes de datos actualmente existentes y la exploración de nuevas fuentes de datos debería realizarse a nivel de los Estados miembros. Si bien, para garantizar la calidad de los datos en toda la UE, conviene establecer normas que garanticen la fiabilidad de los grandes conjuntos de datos. Las tareas de difusión y seguimiento de la adhesión a estos estándares de calidad en los Estados miembros deben ser funciones asumidas por los responsables de datos sanitarios (ver apartado 3.4.1.7.).

La vinculación de diversas fuentes de datos sanitarios debe garantizarse dentro y entre los Estados miembros. Para la mejora continua de la investigación científica se hace necesario expandir y explorar nuevas fuentes de Big Data en salud, a la vez que se asegura tanto su calidad y como su seguridad. Por ello se recomienda adaptar y ampliar las fuentes existentes de Big Data (como, por ejemplo, repositorios de datos en hospitales), de forma que incluyan información necesaria aún no captada (como, por ejemplo, datos biomédicos) y se puedan complementar con nuevas fuentes. La evaluación de las fuentes de datos disponibles y su infraestructura deben tener prioridad para asegurar una exploración específica de nuevas fuentes de datos (como, por ejemplo, dispositivos de salud, redes sociales, etcétera). La atención ambulatoria y la atención primaria, además de diferentes ámbitos de la atención sanitaria (de carácter social, laboral, ambiental, etcétera) deben ser tenidos en consideración en la expansión y exploración de nuevas fuentes de datos.

3.4.1.4. Intercambio abierto de datos.

Se trata de alentar el uso abierto y el uso compartido de Big Data pero sin comprometer los derechos de los pacientes a la protección de su información más personal. El acceso a fuentes complementarias de Big Data permite una mejor comprensión analítica y facilita el análisis de datos, es por ello que se recomienda apoyar el uso abierto y seguro y el intercambio de datos gubernamentales, y datos de diferentes proveedores de atención médica para la investigación de interés público, a nivel nacional e internacional.

El intercambio abierto de datos debe ir acompañado de un marco común con directrices para los procesos operativos. Debería desarrollarse **no sólo a nivel de la UE, sino a nivel mundial**, teniendo en cuenta, por ejemplo, el Libro Blanco de la Global Alliance for Genomics and health (GA4GH) sobre el intercambio responsable de datos genómicos y clínicos[167]. En este marco debe abordar los intereses de todas las partes interesadas y reconocer las diferentes culturas en materia de protección de datos en distintos países, para garantizar un apoyo amplio. El marco debe abordar explícitamente la administración de los datos y la propiedad de los datos, y la seguridad de los datos, además de determinar los requisitos tecnológicos para garantizar un intercambio seguro de datos. En general deben incluirse todos los **elementos pertinentes del uso del Big Data**, como son el acceso a los datos, la seguridad de los datos, la calidad de los datos, la fiabilidad y la integridad de los datos, el formato y las normas (también vinculadas a la acreditación), los procesos de intercambio y la exploración de las posibilidades de extracción automatizada.

[167] GA4GH. Creating a Global Alliance to enable responsable sharing of genomic and clinical data. Recuperado de https://genomicsandhealth.org/files/public/White%20Paper%20June%203%20final_0.pdf. Último acceso 10 enero 2017.

3.4.1.5. Aplicaciones y propósitos.

El Big Data en salud debe aplicarse teniendo bien presente el objetivo; la medicina personalizada es un buen ejemplo para apreciar **el valor añadido que genera**. Se trata de que las aplicaciones estén orientadas al análisis del Big Data en salud, basadas en las necesidades e intereses de las partes interesadas, incluidos los pacientes. A medida que varían los intereses de las partes interesadas, se recomienda expandir y abrir en nuevos campos de aplicación (como, por ejemplo, la vigilancia de infecciones, investigación biomédica, etcétera). La implementación a nivel de los Estados miembros se puede facilitar por medio de subvenciones para aplicaciones del Big Data en salud.

Se trata de obtener información fiable, siempre importante para superar las preocupaciones relacionadas con la aplicación del Big Data en un área sensible como es la salud. Por lo tanto, es recomendable identificar a las partes interesadas que podrían beneficiarse del Big Data en salud, y valorar sus necesidades. Las áreas para aplicaciones del Big Data se deben desarrollar de acuerdo a las necesidades de las partes interesadas y el asesoramiento de expertos a nivel de la UE, a través de una plataforma de diálogo abierto.

3.4.1.6. Análisis de datos.

El poder predictivo del Big Data y la capacidad de integrar datos clínicos (como son, por ejemplo, los datos biomédicos y genómicos) con datos contextuales y del mundo real, ofrecen la posibilidad de que el desarrollo de un análisis de alta calidad genere información de salud que sea fiable y válida. Se trata por tanto de identificar es potencial del análisis del Big Data, mejorar los métodos analíticos y facilitar el uso de métodos analíticos nuevos e innovadores.

Se sugiere que expertos de análisis del Big Data a nivel de Estados miembros puedan desarrollar nuevos métodos analíticos y herramientas, para mostrar su potencial en estudios piloto. Los funcionarios de datos sanitarios que se designen a nivel nacional (ver 3.4.1.7.) y la Comisión Europea deben facilitar este desarrollo mejorando la sensibilización sobre la necesidad de enfoques analíticos actualizados mediante una estrategia de comunicación adecuada (ver 3.4.1.1.) y proporcionando recursos financieros para la investigación (3.4.1.9.).

Es recomendable mejorar y actualizar constantemente los métodos analíticos y las herramientas existentes, para aprovechar plenamente este potencial. Por otro lado, conviene facilitar su desarrollo y uso (como, por ejemplo, la minería de datos, los laboratorios vivos y valiosos repositorios de datos abiertos), considerando el uso práctico del Big Data. Se recomienda establecer y autorizar un comité de investigación

independiente y / o un consejo revisor independiente cuando los nuevos enfoques analíticos no estén suficientemente cubiertos por el marco ético coexistente (como puede ser, por ejemplo, el método In Silico en los ensayos clínicos en investigación medica o tratamientos personalizados).

3.4.1.7. Gobernanza del acceso a los datos y su uso.

Para aprovechar todo el potencial del Big Data en salud, se debe permitir el procesamiento y el uso secundario de datos (que el RGPD facilita) para fines de investigación sanitaria y estadística. Sin embargo, conviene supervisar el fin y la calidad del Big Data en materia de Salud. Se sugiere por lo tanto definir las funciones y responsabilidades en relación con el acceso y procesamiento del Big Data en salud, así como para desarrollar definiciones básicas de datos relevantes en la gobernanza de la salud (como, por ejemplo, usos secundario, casos de tarjetas de donantes de datos) en forma de un **glosario para fomentar un lenguaje común**.

Se debe nombrar en cada Estado miembro a los denominados *health data officers* para supervisar y coordinar las actividades nacionales desde la perspectiva de la salud pública. Estos profesionales de datos sanitarios deberían establecerse dentro de los marcos nacionales existentes y deberían colaborar con las autoridades de protección de datos y los comités de ética ya existentes a nivel nacional. Debe establecerse una plataforma a escala europea, para el diálogo regular entre estos responsables de datos sanitarios para abordar cuestiones relativas a sus tareas, como la de asegurarse que las aplicaciones de salud se basan estrictamente en la evidencia y no sólo están diseñadas en el mero interés de las empresas del mercado.

Se trata pues de implementar **mecanismos de gobernanza para garantizar el acceso y el uso de forma segura y justa del Big Data para la investigación en salud**. Estos mecanismos de gobernanza deben ser transparentes y justos. El tratamiento y la vinculación de las fuentes de datos, así como el acceso y el uso secundario, deberían ser aprobados por revisores independientes para garantizar un acceso y un uso de datos no discriminatorios y adecuados. Para facilitar esto, los responsables nacionales de datos sobre salud deberían coordinar el proceso de gobernanza y fomentar la cooperación entre los diferentes propietarios de bases de datos y las partes interesadas. Con el fin de agilizar la gobernanza de las diferentes fuentes de datos de manera segura, debería ponerse a disposición a nivel nacional una plataforma para vincular y acceder con seguridad a los datos procedentes de diferentes fuentes.

La aplicación de los mecanismos nacionales de gobernanza para el Big Data en salud a escala de la UE puede apoyarse en la orentación sobre el proceso de aprobación de acceso a datos y la implementación técnica de plataformas de datos, como por ejemplo, proporcionando información sobre **modelos de buenas prácticas para la gobernanza de los datos** a nivel de investigación (como, por ejemplo, el Consorcio

Epigenoma Humano, IHEC). Las directrices y los procedimientos operativos armonizados en toda la UE garantizan que las normas para el acceso a los datos sean similares en los distintos países y que sea posible la interoperabilidad de los componentes técnicos.

3.4.1.8. Normalización.

La agrupación, el intercambio y el análisis de datos se hacen más eficientes a través del establecimiento de estándares comunes mediante de la cadena de valor del Big Data en salud. Por lo tanto, se recomienda adoptar o desarrollar, en su caso, normas de alcance internacional que abarquen el aspecto de la interoperabilidad (prioridades de normalización de las TIC para el mercado único digital[168]), como, por ejemplo, en temas de consentimiento del paciente en el uso del Big Data en salud, nomenclatura de genotipos o asuntos de ética. Se trata de desarrollar estándares para Big Data en salud, con el fin de mejorar y simplificar su aplicación, así como **mejorar la interoperabilidad.**

La mejora de la interoperabilidad incluye la normalización y armonización del contenido básico y la estructura de las formas de consentimiento del paciente, donde se pueden abordar distintos modelos de consentimiento (como, por ejemplo, consentimiento dinámico, o consentimiento ampliado) y también los consentimientos digitalizados para facilitar el uso secundario de los datos y el intercambio de datos. La diversidad de los formatos de los datos y su representación dificultan la combinación de conjuntos de datos procedentes de diferentes fuentes, motivo por el cuál la introducción de estándares puede mejorar la interoperabilidad de diferentes formatos de datos, conjuntos de datos y almacenes de datos (por ejemplo, ELIXIR -ver apartado 2.1.4.-).

3.4.1.9. Financiación y recursos financieros.

Se recomienda que las instituciones de la UE apoyen financieramente iniciativas a nivel nacional, informando acerca de las iniciativas nacionales existentes de Big Data en los Estados miembros y emitiendo directrices o **ejemplos de buena prácticas** para un uso eficiente, que por otro lado mejore los resultados del Big Data en salud, para beneficio de todos los ciudadanos. Se sugiere que se faciliten recursos para el establecimiento de un organismo coordinador (a nivel de la UE) que oriente y supervise estas actividades. Se trata de garantizar que la Comisión Europea se comprometa a realizar una inversión decidida que garantice la rentabilidad y la sostenibilidad de la misma.

[168] Comisión Europea, comunicado al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *ICT Standardisation Priorities for the Digital Single Market.* Obtenido de https://ec.eu- ropa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market. Último acceso 22 enero 2017.

Con la finalidad de distribuir la carga financiera inicial y el riesgo de la inversión, se sugiere la financiación a través de múltiples fuentes (bien sean asociaciones público-privadas o público-público), las organizaciones a nivel de la UE deben invertir en desarrollar grandes sistemas de datos, una **infraestructura compartida de gestión de datos** y un sistema de comunicación. (ver el apartado 3.4.1.3.), para lo cual se tienen que incentivar las inversiones nacionales en infraestructuras mejoradas para el procesamiento de los datos sanitarios y las asociaciones continuas entre las distintas partes interesadas. Las inversiones en Big Data en salud deben eventualmente generar retornos sociales y económicos sostenibles, para toda la sociedad.

3.4.1.10. Aspectos legales y normas de privacidad.

Se recomienda que la Comisión Europea apoye la aplicación práctica de la nueva legislación, por ejemplo, a través de la convocatoria de debates entre las autoridades nacionales de protección de datos y los interesados en el sector sanitario, sobre la interpretación antes de la aplicación efectiva del RGPD; la privacidad y la protección de datos quedan bien definidos en la UE, con normas claras y coherentes, en materia de gestión y control de datos, y este RGPD refuerza los derechos de las personas y armoniza las legislaciones nacionales. Este Reglamento se complementa con la Directiva sobre seguridad de los sistemas de red y de información (Directiva NIS), que introduce medidas jurídicas para aumentar el nivel de ciberseguridad y la cooperación de los Estados miembros en esta cuestión.

Para proporcionar seguridad al generar, acceder y compartir Big Data es preciso un marco legal de Big Data en salud que esté claramente definido y sea consistente. Se recomienda aclarar y alinear la regulación legal en general y de privacidad en particular, sobre Big Data en salud. Se trata por lo tanto de aspectos como la titularidad de los datos, la confidencialidad de los datos y el consentimiento del paciente, además de otros aspectos legales como el almacenamiento (como, por ejemplo, en la nube) y el procesamiento de datos, así como los fundamentos legales para la reutilización y la transferencia internacional de datos, el uso secundario de datos de salud (como, por ejemplo, a través de la introducción de tarjetas de donantes de datos).

Así pues, resulta vital entender qué se puede extraer de este estudio para esta investigación, y es que el estudio ofrece directrices para el desarrollo futuro de una cadena de valor del Big Data de la UE en el ámbito de la salud, en nombre, entre otros, de los miembros de la *eHealth Network*[169], a saber, los 28 con

[169] El Artículo 14 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, define los objetivos de la *eHealth Network*, a saber:

"a) esforzarse para conseguir unos beneficios económicos y so ciales sostenibles merced a sistemas y servicios europeos de sanidad electrónica y a aplicaciones interoperables que per mitan alcanzar un alto grado de confianza y seguridad, me jorar la continuidad de los cuidados y garantizar el acceso a una asistencia sanitaria segura y de calidad;

b) elaborar directrices en relación con:

Noruega (Ministerio de Sanidad) como observador[170]. Así, básicamente, los responsables políticos se enfrentan a los desafíos del Big Data en salud, como la necesidad de adoptar las regulaciones y marcos existentes para las nuevas tecnologías, pero también los referidos a la mentalidad de las personas; por lo que resulta crucial **involucrar a grupos de pacientes** pues sólo con su participación, las posibilidades de cambiar la mentalidad pública hacia el Big Data en el ámbito de la salud se puede garantizar. Puesto que la salud es un bien especial, y los estándares éticos son especialmente exigentes en este campo, es necesario un enfoque innovador, cuidadoso y sensible.

El estudio muestra claramente la existencia una **amplia variedad de iniciativas y emprendimiento** en el área, desde herramientas únicas pero complejas de detección genómica hasta la definición de un conjunto mínimo de datos, para el intercambio entre países de datos de pacientes, en una industria todavía en crecimiento como son las aplicaciones móviles de salud y bienestar.

Se precisa con urgencia aplicar políticas de sensibilización sobre el **valor añadido del Big Data en salud**, como se apunta el apartado 3.4.1.1., una estrategia de comunicación para fomentar una mentalidad pública positiva hacia la aplicación del Big Data en salud, que fomente un diálogo abierto y de mejora continua. Desde enfermedades crónicas, nutrición, diagnóstico de cáncer o su tratamiento, etcétera, todos se pueden beneficiar, a la vez que otro hallazgo importante del estudio es que se debe garantizar la **interoperabilidad jurídica**, con referencia a la aplicación práctica del RGPD.

3.4.2. El camino hacia la armonización.

La globalización ha tenido importantes consecuencias en la autonomía de los gobiernos nacionales, **conduciendo los ordenamientos jurídicos de las democracias económicamente más robustas y maduras hacia la convergencia** de manera muy significativa (Kagan, 2007); un contexto económico internacional cada vez más integrado y competitivo, junto a los actuales cambios demográficos, han llevado a estas democracias del bienestar a enfrentarse a retos similares representados por sus problemas sociales, económicos, políticos y medioambientales. La UE y los tratados internacionales exigen una armonización

---

i) una lista no exhaustiva de datos que deberán incluirse en el historial de los pacientes y podrán ser compartidos por los profesionales sanitarios para propiciar una continui dad en los cuidados y la seguridad de los pacientes a través de las fronteras, y

ii) unos métodos eficaces que permitan utilizar los datos médicos en beneficio de la salud pública y la investiga ción;

c) apoyar a los Estados miembros para que impulsen medidas comunes de identificación y autenticación para facilitar la transferibilidad de los datos en la asistencia sanitaria trans fronteriza.

Los objetivos contemplados en las letras b) y c) se perseguirán con la debida observancia de los principios de protección de datos tal y como se encuentran establecidos en las Directivas 95/46/CE y 2002/58/CE".

[170] Comisión Europea. *eHealth Network*. Recuperado de: https://ec.europa.eu/health/ehealth/policy/network_es. Último acceso 23 enero 2017.

transnacional de leyes nacionales referidas a aspectos importantes como los derechos humanos, la salud pública, la propiedad intelectual, el control de la contaminación, la seguridad de los bancos, etcétera.

Ya señalaba Simmons (2001) que en un mundo cada vez más interdependiente, cuando sistemas políticos poderosos como EE.UU. y la UE empiezan a sufrir importantes costes o inconvenientes derivados de las leyes y prácticas nacionales divergentes, entonces resulta probable que utilicen instituciones internacionales o supranacionales (junto con su propio sistema económico y político) para **empujar a otras naciones a adoptar sus propios estándares legales**, lo de la política poderosa.

No son pocos los retos, la Europa de los 27[171] ha implementado la Directiva 95/46/CE 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, de forma diferente, las divergencias entre la legislación de protección de datos de los Estados miembros de la UE son consecuencia de la presencia en la Directiva de cláusulas abiertas. Pero a pesar de la distinta aplicación de la normativa por las autoridades de control y la disparidad de instrumentos coercitivos, la armonización plena está en camino, a través de la jurisprudencia[172] y del nuevo RGPD; por otro lado, esta nueva legislación para la armonización, creen algunos investigadores, puede poner serias trabas a la investigación epidemiológica y médica en general (Ploem, Essink-Bot y Stronks, 2013).

El artículo 7 f) de dicha Directiva[173] establece que los Estados miembros dispondrán que el tratamiento de datos de carácter personales sólo pueda efectuarse, entre otros supuestos, si "es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"[174].

Por otro lado, el TJUE[175] define el alcance normativo de la norma señalando que no admite que, en ausencia del consentimiento del interesado, las normativas nacionales exijan (para permitir el tratamiento de datos de carácter personal "necesario para la satisfacción de un interés legitimo"), además del respeto de los derechos y libertades fundamentales del interesado, que los datos se encuentren siempre en fuentes accesibles al público, "excluyendo así de forma categórica y generalizada todo tipo de tratamiento de datos

[171] Hoy 28 con Croacia.

[172] El Tribunal de Justicia de la Unión Europea resolvió el 24 de noviembre de 2011 las cuestiones prejudiciales planteadas por el Tribunal Supremo relativas a la interpretación del artículo 7 f) de la Directiva 95/46/CE, 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.

[173] La Sentencia proclama que el artículo 7f) tiene efecto directo.

[174] Derechos a la intimidad y a la protección de datos personales, incluidos en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

[175] Tribunal de Justicia de la Unión Europea.

que no figuren en tales fuentes". Sin embargo la mera invocación de un interés legítimo no debe considerarse suficiente para legitimar el tratamiento de datos de carácter personal sin el consentimiento del afectado.[176][177]

Al mismo tiempo la Sentencia señala que "el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate", y deja claro que en este marco "la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado", permitiendo que a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46/CE, "los Estados miembros establezcan los principios que deben regir dicha ponderación".

Entre los criterios de ponderación, la Sentencia se refiere al hecho de que los datos no se encuentren en fuentes accesibles al público, recordando que "a diferencia de los tratamientos de datos que figuran en fuentes accesibles al público, los tratamientos de datos que figuran en fuentes no accesibles al público implican necesariamente que el responsable del tratamiento y, en su caso, el tercero o terceros a quienes se comuniquen los datos, dispondrán en lo sucesivo de ciertas informaciones sobre la vida privada del interesado. Esta lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos."

Se investiga si una regulación unificada en materia de protección de datos mejoraría la seguridad de los pacientes, la calidad de los datos, fortaleciendo los derechos de los individuos y definiendo procedimientos de control de calidad; no todos los investigadores están de acuerdo en que este tipo de iniciativas supongan una mejora efectiva[178].

En todo caso parece que la armonización integral está lejos en opinión de algunos autores, como es el caso de Giménez (2015) de acuerdo con sus "Propuestas ante un futuro incierto para la protección en la

[176] En los fundamentos de la Sentencia, el propio Tribunal precisa la interpretación que debe darse a dicho artículo, subrayando la necesidad de realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes.

[177] La Sentencia recuerda que el artículo 7 f) de la Directiva "establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado".

[178] Herveg (2014), "Data Protection and the Patient's Right to Safety".

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?"; los Estados miembros de la UE no disponen de reglas comunes para establecer la ley aplicable en materia de responsabilidad civil extracontractual en el ámbito de los litigios privados internacionales derivados de la vulneración del derecho fundamental a la protección de datos, así pues cada Estado miembro aplica sus propias normas autónomas, con diferentes soluciones dependiendo si el proceso se desarrolla en un Estado miembro o en otro. Estas circunstancias acarrean un serio riesgo de *legal shopping* y una clara inseguridad jurídica en las relaciones privadas internacionales. La armonización comunitaria en lo relativo a las normas de conflicto haría posible la protección en la UE del titular del derecho a la protección de datos de carácter personal ante una transferencia internacional de datos ilícita. Giménez (2015) pone de manifiesto que el legislador comunitario no puede permanecer indiferente, y debe buscar una alternativa que sea viable, alcanzar un punto de encuentro entre los diversos intereses presentes, de forma que se facilite un acuerdo de consenso entre los Estados miembros; esta disparidad de posibles soluciones conlleva la búsqueda de una armonización material, por mínima que sea posible, que asegure en todos los Estados miembros un "estándar de protección adecuado" a los potenciales o eventuales perjudicados.

La protección de datos como derecho fundamental que resulta ser imprescindible en una sociedad moderna y avanzada (aunque pueda considerarse que el derecho a la protección de datos esté consolidado en países como España y en la UE en general), debe continuar con su consolidación, por lo que hay que estar en alerta permanente, para lograr la **normalización de la cultura de la protección de datos que defiende** Mañas (2009).

Auffray et al. (2016) abordan los aspectos legales y regulatorios del uso de Big Data en el terreno de la investigación; un aspecto crucial que abordar se refiere a la aceptación de regulación de Big Data para la evaluación de nuevas terapias farmacológicas o biológicas para complementar grandes ensayos clínicos. Que los proyectos piloto de colaboración entre universidades y hospitales no cuentan con los procedimientos establecidos para capturar de manera efectiva y compartir datos con otras organizaciones y países. Auffray et al. (2016) defienden con acierto que **tenemos que desarrollar y adoptar estándares de alta calidad** para la generación y procesamiento de datos, como medio para asegurar que los datos más significativos y válidos con una semántica bien determinada sean procesados correctamente y compartidos. La calidad de la generación de datos, así como la aceptación del tratamiento y la reglamentación del Big Data son actualmente una materia de relevancia internacional; sirvan de ejemplo iniciativas de investigación como el International Cancer Genome Consortium (ICGC), el International Human Epigenome Consortium (IHEC), el Genemoic Standard Consortium (GSC), y el Clinical Data Interexchange Standards Consortium (CDISC)

y diversos comités técnicos (TC[179]) de normalización de ISO[180] (International Organization for Standardization) como, por ejemplo, ISO/TC276, referido a la biotecnología, cuyo grupo de trabajo WG 5 (*working group 5*) trata específicamente el procesamiento e integración de datos.

El 30 de noviembre se ha establecido como el día internacional de la seguridad de la información. El *international information security management system* (ISMS) o sistema de gestión de seguridad de la información (SGSI) define la norma ISO/IEC[181] 27001, que es la herramienta más empleada en todo el mundo para gestionar adecuadamente la información[182]. Esta norma y la ISO/IEC 27002 representan las únicas certificaciones internacionales que definen los requisitos para un **sistema de seguridad de la información de acuerdo con ISO**, y los controles y objetivos del sistema de seguridad de la información, respectivamente. Estas normas proporcionan un marco para gestionar los riesgos de la seguridad de la información y facilita el cumplimiento normativo en materia de protección de datos. La norma ISO/IEC 27018 se refiere a la protección de la información de los clientes, es decir, a la seguridad de la información de identificación personal (PII[183]) en sistemas cloud[184], es decir, establece requisitos que garanticen "que los proveedores de servicios en la nube puedan ofrecer controles adecuados de seguridad de la información"[185]; **se espera un alineamiento cada vez mayor de las normas ISO con el Ordenamiento de la UE** y la definición de un procedimiento de certificación específica de su aplicación efectiva por las organizaciones, sin perjuicio de las auditorías que realicen terceros, independientes, de acuerdo con otros estándares. Esta norma ISO/IEC 27018 **se basa en leyes y regulaciones de la UE**, por lo que se acomoda al modelo europeo de protección de datos de carácter personal, ofrece confianza para los proveedores (que decidan someterse a ella) sobre su capacidad de cumplimiento normativo[186] al establecer unas *"security techniques"* (medidas o controles de seguridad) y *"code of practice"* (código de buenas prácticas). Anteriormente los proveedores de nube pública sólo podían certificarse, en cuanto a seguridad, a través de las normas ISO 27001 (antes mencionadas), pero desde la perspectiva de la gobernanza de las tecnologías de la información y de la

[179] Acrónimo del inglés "*technical committee*".

[180] La Organización Internacional de Normalización se fundó en 1946 con delegados de 25 países reunidos en el Instituto de Ingenieros Civiles de Londres, quiénes crearon esta organización internacional para facilitar la coordinación internacional y la unificación transfronteriza de las normas industriales. Desde entonces ISO ha redactado más de 21.000 normas internacionales que abarcan la tecnología y la fabricación. Hoy tiene 163 países miembros. Su sede está en Ginebra, Suiza. Debido a que esta Organización Internacional de Normalizació tennía diferentes acrónimos en distintos idiomas los fundadores acordaron que el nombre de la organización sea ISO, denominación que deriva del griego *"isos"*, que quiere decir "igual". (ISO. Recuperado de http://www.iso.org/iso/home/about.htm . Último acceso 1 enero 2017).

[181] ISO ha formado varios comités técnicos conjuntos, con la International Electrotechnical Commission (IEC), para desarrollar normas y terminología relacionadas con tecnología eléctrica y electrónica; ISO/IEC JTC 1 desarrolla normas en el campo de la tecnología de la información y de la tecnología de la información y la comunicación.

[182] AENOR (noviembre 2016).

[183] Acrónimo del inglés "personally identifiable information".

[184] Arteaga (2014) aborda la ventajas e inconvenientes de crear nuevos modelos más rentables como el *cloud computing*, que permite un almacenamiento de una enorme cantidad información y datos, a través de técnicas que ofrecen un ahorro en coste y tiempo, acompañado de una gestión más eficiente y flexible de los recursos, la oportunidad de compartir servicios y especialmente la interoperabilidad de los datos.

[185] Análisis de la norma ISO/IEC 27018. Recuperado de http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal. Último acceso 2 enero 2017.

[186] ISO/IEC 27018:2014. Recuperado de http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498. Último acceso 2 enero 2017.

responsabilidad en el tratamiento de los datos personales no existían parámetros internacionalmente reconocidos respecto de la privacidad, ahora con la ISO 27018 se puede saber si el proveedor de servicios en la nube pública ha tomado medidas de protección de datos personales, que se pueden auditar y verificar por terceros, y lo que es más importante, ayuda al proveedor a cumplir con sus obligaciones en el área de la protección de datos (Fernández y Recio, 2015).

Auffray et al. (2016) insisten en los principios FAIR[187] (que se identifican con facilidad de localización, accesibilidad, interoperabilidad y reutilización) para la gestión de datos científicos, pues debe ayudar a todos los actores (incluyendo el mundo académico) para obtener beneficios inmediatos, también en el campo de la salud; dada la complejidad de los variados tipos de datos y el elevado número de actores involucrados en la implementación de estándares de datos, la mayor posibilidad de éxito creen debe ir acompañada de **proyectos piloto concretos**. Así por ejemplo, existen nuevas iniciativas que fomentan el intercambio de datos clínicos como la Alianza Mundial para la Genómica y Salud[188], que trabaja para la armonización de los marcos técnicos, éticos y legales. Rodríguez-Iglesias et al. (2016) también apoyan la aplicación de los principios FAIR a la publicación de datos científicos, a la vez que Lévy (2010) habla del *Information Economy MetaLanguage* -IEML-, como nuevo métodos para la interoperabilidad semántica, algo necesario para la armonización internacional.

En este sentido ISO desempeña un papel importante en el terreno internacional (no solamente en Europa); **normas como ISO/IEEE[189] 11073[190],** que incluye un grupo de normas relativas a *eHealth*, avanzan por este camino en la buena dirección, la armonización e integración de estándares; se trata de normas referidas a "personal health data" o datos de salud de carácter personal, y consiste en un conjunto de normas que abordan la interoperabilidad de dispositivos personales de salud (PHDs[191]) como balanzas de peso, monitores de presión sanguínea, monitores de glucosa en sangre, etcétera; normas que inciden especialmente en dispositivos para el uso personal y en un modelo de comunicación más sencillo. Habrá que atender a las organizaciones que tratan la interoperabilidad de dispositivos médicos, que al margen de ISO e IEEE, son CEN[192] en Europa y AENOR[193] (anteriormente IRANOR[194]) en España. El Acuerdo de Viena se

[187] Acrónimo del inglés *"findability", "accessibility", "interoperability",* y *"reusability"*.

[188] En inglés *"Global Alliance for Genomics and Health"*.

[189] Acrónimo del inglés "*Istitute of Electrical and Electronics Engineers*", e incluye IEEE *Engineering in Medicine and Biology Society*.

[190] ISO/IEEE 11073-10418:2014. Recuperado de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61897. Último acceso 2 enero 2017.

[191] Acrónimo del inglés "*personal health devices*".

[192] El Comité Europeo de Normalización es el principal creador de normas europeas y especificaciones técnicas, reconocido de acuerdo con la Directiva 98/34/CE para la planificación, elaboración y adopción de normas europeas. Creado como una organización internacional privada sin ánimo de lucro, con sede en Bruselas, el CEN es un facilitador de negocios en Europa, a través del desarrollo de sus funciones ayuda a eliminar las barreras comerciales entre la industria europea y los consumidores, y fomenta la economía europea en el comercio mundial, el bienestar de los ciudadanos europeos y el medio ambiente. A través de sus servicios que proporciona una plataforma para la armonización y el desarrollo de normas paneuropeas.

[193] Asociación Española de Normalización y Certificación.

firmó entre el CEN e ISO en 1991, y entró en vigor a mediados de los años 2000, con el objetivo fundamental de evitar una duplicidad de normas que pudieran entrar en conflicto, entre el CEN y la ISO. En la última década este acuerdo ha tenido un impacto positivo en la consecución de su objetivo puesto que el CEN ha adoptado una serie de normas ISO que han sustituido a las correspondientes normas CEN.

La armonización técnica es importante pero la armonización de los marcos regulatorios es crucial para el intercambio de datos, como defienden Auffray et al. (2016), para garantizar la protección de los datos de carácter personal y el cumplimiento de las normas vigentes, que incluyen disposiciones sobre cómo prevenir, tratar y perseguir cualquier infracción. Auffray et al. abordan la protección de la privacidad y las políticas de intercambio de datos para concluir que existen amplias diferencias dentro y fuera de Europa con respecto a la protección de la privacidad y a la política de cesión de datos. El Proyecto de Reglamento europeo de protección de datos de 2012[195] (hoy ya una realidad) debe armonizar, en opinión de Auffrey at al., la fragmentación actual en la UE bajo la Directiva 95/46/CE de protección de datos de carácter personal.

La **certificación es una herramienta de autorregulación o corregulación** que puede solventar todos los conflictos que se pueden generar a raíz de fallos en seguridad y eficiencia que afectan de manera directa a los derechos fundamentales de los consumidores y usuarios, como es el derecho a la protección de datos, algo que defiende muy acertadamente Cordero (2016), aunque para ello se hace necesario el respaldo de todas las partes interesadas, incluidos fabricantes y las organizaciones de consumidores; en el marco europeo hay dos mecanismos que recoge Cordero en este sentido: (1) el nuevo RGPD (sección 5) que apuesta por la implementación de medidas proactivas para ofrecer protección a los derechos de los usuarios, como alternativa al excesivo desarrollo normativo, ya que tienen la capacidad de adaptarse con mayor facilidad y eficiencia al desarrollo tecnológico (2) la Comisión Europea incentiva desde 2007 (a través del 7º Programa Marco de Investigación y Desarrollo[196]) el estudio e implementación de mecanismos de certificación a partir de los cinco criterios de evaluación del paquete "Legislar mejor"[197] (eficiencia, eficacia, coherencia, pertinencia y valor añadido de la UE).

---

[194] El Instituto de Racionalización y Normalización fue creado el 11 de diciembre de 1945 por el Consejo Superior de Investigaciones Científicas, bajo el patronato de Juan de la Cierva. IRANOR comenzó a aprobar las primeras normas españolas (UNE -siglas de "una norma española"-), armonización de las prescripciones internacionales. La Dra. Marina Kress Voltz fue Directora de Relaciones Internacionales de IRANOR durante su etapa de mayor desarrollo, contribuyendo significativamente a la armonización de la normativa europea, precisamente coincidiendo con la incorporación de España a la Comunidad Económica Europea, en 1986. A partir de este año, las actividades de normalización y certificación pasaron de IRANOR a la entidad privada AENOR.

[195] Consejo de la UE (11 junio 2015). *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).* Recuperado de http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Último acceso 7 diciembre 2015.

[196] Reemplazado por el Programa Horizonte 2020, el mayor programa de investigación e innovación de la UE, en vigor desde 2014 hasta 2020, con un presupuesto de ca. €80.000 millones con el objetivo es asegurar la competitividad global de Europa.

[197] El 13 de abril de 2016 se firma el Acuerdo Interinstitucional entre el Parlamento Europeo, el Consejo de la UE y la Comisión Europea sobre la mejora de la legislación, cuyo considerando no.3 indica "Las tres Instituciones recueran la obligación de legislar únicamente y en la medida en que sea necesario, de conformidad, con el artículo 5 del Tratado de la Unión Europea sobre aplicación de los principios de subsidiariedad y proporcionalidad".

Algun autor[198] (teórico de la convergencia), cuya opinión no comparto, hablan de una supuesta **"americanización"[199] del derecho en Europa occidental**; su planteamiento es que la competencia global, la UE y la agresividad de empresas y bufetes de EE.UU. estarían forzando o induciendo a países europeos a emular las leyes estadounidenses (neoliberales) y a adoptar formas de gobernanza contenciosas, que fomentan la litigiosidad, propias de EE.UU., erosionando así las políticas legislativas propias del modelo europeo[200], y aumentando los costes. Kagan (2007) cree que esta tendencia es firme aunque cuestiona con determinación hasta donde puede llegar la convergencia con la normativa estadounidense, en particular en lo que respecta a los países europeos, en función de sus sistemas e instituciones jurídicas. Kagan sugiere que en todas las naciones europeas existen facciones políticas, grupos de interés y élites jurídicas que estarían en desventaja al adoptar leyes y formas legales que son propiamente norteamericanas, y que batallan contra dicha "americanización" o tratan de suavizarla, adaptándola a las tradiciones jurídicas y administrativas de los países europeos. Para Kagan existen reformas jurídicas propuestas en Europa tendentes a seguir un modelo norteamericano, pero con la advertencia de ser cuidadosos para no acabar con un modelo como el de EE.UU., concluyendo que, aunque los países europeos pueden seguir creciendo en niveles de litigiosidad, no han adoptado y probablemente no adopten nunca sistemas contenciosos que puedan asemejarse al método estadounidense.

A la luz del actual envejecimiento de la población, que se enfrenta a la percepción de amenaza de una vigilancia permanente en la red, se deben tener en cuenta las necesidades y expectativas de los usuarios finales; por ello se exige una estrecha colaboración entre las partes implicadas, que podría facilitar el proceso integral de armonización en materia salud, como bien apuntan Haluza y Jungwirth, 2015.

3.4.3. Interoperabilidad.

En 2010 ya presentó la Comisión Europea un informe sobre las ventajas de la interoperabilidad en *eHealth*[201], definiendo cómo para alcanzar los máximos beneficios derivados del *eHealth* se imponía la conectividad y el acceso seguro a la información.

En 2011 se adopta la primera ley de la UE con provisiones sobre la interoperabilidad en materia de *eHealth*, la Directiva sobre los derechos de los pacientes en atención sanitaria más allá de las fronteras, pero antes, el 1 de julio de 2008, se lanza epSOS ("*Smart Open Services for European Patients*"), un proyecto

[198] En esta línea se posiciona Kagan, 2007.

[199] Concepto que debe ser entendido como referido a los EE.UU. exclusivamente, y no a otros países de América, en este caso.

[200] Garth y Dezelay, 1995; Kelemen y Sibbitt 2004; Kelemen 2006.

[201] Comisión Europea. Interoperable eHealth is worth it. Recuperado de http://www.ehr-impact.eu/downloads/documents/ehr_impact_study_final.pdf. Último acceso 9 enero 2017.

europeo de *eHealth*, con el fin de alcanzar la interoperabilidad de los servicios de *eHealth*, que facilite un sistema integrado de salud (Linden, 2009). Se trata de un proyecto de apoyo a la política de las TIC, mediante el cual las soluciones técnicas contribuyen al intercambio de información de pacientes entre distintos países. Una de las prioridades del proyecto es garantizar la protección de las historias clínicas, cumpliendo con la legislación de la UE como la legislación nacional de cada país en materia de protección de datos. Se trata de un proyecto para promover la cooperación entre Estados miembros de la UE en el ámbito sanitario, una cooperación que contribuya a establecer una estructura común de sistemas sanitarios diferentes que sea más eficiente. Cada vez existen más pacientes desplazados en la UE, pacientes que precisan algún tipo de asistencia sanitaria en Estados miembros donde no residen habitualmente; recurrir a un uso conjunto de las tecnologías de la información contribuye a la disponibilidad y a la calidad del tratamiento a dichos pacientes (epSOS).

Esta iniciativa abierta en *eHealth es* un proyecto piloto a gran escala que se centra principalmente en la historia clínica electrónica (*patient summary)* y la prescripción electrónica (*ePrescription*), que abarca el acceso transfronterizo entre 22 países de la UE (Alemania, Austria, Bélgica, Croacia, Dinamarca, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, Luxemburgo, Malta, Polonia, Portugal, Eslovaquia, Eslovenia, España, Suecia, Holanda, Reino Unido y República Checa) y 3 países no comunitarios (Suiza, Turquía y Noruega); donde España ha sido líder con dos autonomías que han englobado más pilotajes que el resto de países participantes juntos[202]. La tabla 4 contiene el cuestionario elaborado para el paciente en el desarrollo de este proyecto, con el objetivo de conocer su opinión sobre algunos aspectos del servicio recibido de acceso a su historia clínica resumida.

[202] Proyecto epSOS. Recuperado de http://www.diariomedico.com/2012/12/26/area-profesional/gestion/proyecto-epsos-espana-es-lider-europeo-tic-salud. Último acceso 12 diciembre de 2016.

Tabla 3.3.
Cuestionario para el paciente sobre historia clínica resumida, proyecto epSOS.

ID	Pregunta	Respuestas
ASPECTOS LEGALES		
1	Creo que la privacidad de mis datos ha sido apropiadamente mantenida.	Completamente en desacuerdo. En desacuerdo. No estoy seguro. De acuerdo. Completamente de acuerdo. No lo sé
2	He dado o confirmado mi consentimiento.	Si No No lo sé
ASPECTOS DEL SERVICIO		
3	¿Ha facilitado el acceso a su Historia Clínica Resumida su comunicación con el profesional de salud?	Si No No lo sé
4	¿Le ha parecido que ha recibido una atención más rápida gracias al servicio de "Historia Clínica Resumida"?	Si No No lo sé
5	El servicio de Historia Clínica Resumida ha sido útil para intercambiar información clínica.	Completamente en desacuerdo. En desacuerdo. No estoy seguro. De acuerdo. Completamente de acuerdo. No lo sé
6	¿Utilizaría el servicio de Historia Clínica Resumida de nuevo?	Si No No lo sé
7	Por favor explique porqué sí o /porqué no	(respuesta abierta)
8	¿Recomendaría el servicio de Historia Clínica Resumida a un amigo o a un familiar?	Si No No lo sé
9	Por favor, explique porqué sí /porqué no	(respuesta abierta)
10	¿Cree que el acceso a la Historia Clínica Resumida constituye una mejora?	Si No
11	¿Cuál es el beneficio más importante del servicio de Historia Clínica Resumida?	(respuesta abierta)

Fuente: tabla de elaboración propia a partir de datos de epSOS

Así, queda patente cómo la Agenda Digital para Europa incluye proyectos y acciones específicas de *eHealth*. A pesar de la crisis económica se prevé que el mercado mundial de *mHealth* crecerá hasta €17.5 billones al año para 2017 según estimaciones de la UE.

En cuanto a la implicaciones reales del Plan 2012-2020, para los profesionales significa más oportunidades para desarrollar y mejorar sus habilidades digitales en áreas de creciente demanda;

incrementará su confianza para trabajar con herramientas electrónicas para la salud, y llevará a una mayor aceptación y uso de las tecnologías de *eHealth*. Para los médicos, esto implica mayor tiempo de calidad con sus pacientes, y menos citas gracias a la eReceta (o receta electrónica) y al seguimiento electrónico. Para pacientes, significa menos esfuerzo, tiempo y recursos destinados a visitas al hospital; por ejemplo, en el Reino Unido desde abril 2013 los pacientes del NHS (National Health System) o Sistema Nacional de Salud pueden solicitar citas y recetas electrónicas. Este paso también permitirá que los pacientes adopten un papel más proactivo en la gestión de su salud.

3.4.4. Gestión de la información.

Hilbert y López (2011) analizaron la capacidad mundial de telecomunicaciones bidireccionales de 1986 a 2007; en este periodo creció un 28% anual, seguido de cerca por el aumento de la información almacenada a nivel mundial, que alcanzó 23%. En cambio, en este mismo periodo temporal la capacidad de la humanidad para la difusión unidireccional de información a través de los canales de radiodifusión (más tradicionales) ha experimentado un crecimiento anual de sólo un 6%. Así confirman que las telecomunicaciones han estado dominadas por las tecnologías digitales desde 1990 y esto es indicativo de la inmensa evolución tecnológica en pocos años.

La naturaleza sensible de la información sobre nuestra salud y el alto nivel de dependencia de los profesionales sanitarios de registros fiables, los problemas de fiabilidad (que los datos que integran el EHR sean precisos y permanezcan precisos), la seguridad (titular y usuarios del EHR pueden controlar la transmisión y el almacenamiento de los dato), y la privacidad (el sujeto puede controlar el uso de los datos y su difusión) son temas que deben ser abordados, de forma directa y efectiva, por organizaciones y profesionales de la salud o relacionadas con la salud. La fiabilidad, la seguridad, y la privacidad se alcanzan a través de la puesta en marcha de políticas preventivas y protectoras, herramientas, y acciones que abordan la protección física, la integridad de los datos, el acceso a fuentes de información, y la protección contra la revelación no autorizada de información; una revisión integral y fuente de referencia sobre la regulación de protección de datos se publicó en la Organización Panamericana de Salud[203].

A pesar del importante papel que los EE.UU. han jugado en las primeras iniciativas internacionales sobre la privacidad de la información, el resto del mundo más bien ha seguido hasta ahora un modelo similar al de la UE , y ha adoptado legislaciones de protección de datos al estilo europeo (Greenleaf, 2012).

[203] Rodrigues R.J., Wilson P, Schanz SJ. 2001. The regulation of privacy and data protection in the use of electronic health information: an international perspective and reference source on regulatory and legal issues related to person-identifiable health databases. In: Essential Drugs and Technology Program, Division of Health Systems and Services Development. Washington, DC: Pan American Health Organisation/World Health Organisation.

Ahora la pregunta es saber si la aprobación del nuevo Reglamento General de Protección de Datos en la UE influirá en otra dirección, qué impacto tendrá; la nueva regulación europea vía reglamento es vista por algunos autores como un riesgo que amenaza con desestabilizar la actual política de acercamiento y colaboración entre la UE y EE.UU., al sustituir al actual equilibrio con derechos individuales reforzados y una mayor centralización del control (Schwartz, 2013).

Para Kankanady y Wells (2013) la gestión de la información puede suponer un esfuerzo inagotable tanto para el personal sanitario como para los legisladores en materia sanitaria; el sector de la salud por su naturaleza requiere una especial atención a la clasificación de la información y a la arquitectura de dicha información. La importancia de la gobernanza de la información es objeto de estudio por distintos investigadores hoy en día, puesto que se está convirtiendo en un tema cada vez más valioso para la gestión de la información sanitaria. Los datos personales son parte intrínseca de la información sanitaria que debe gestionarse, tarea por lo tanto que deviene aún más compleja. Se recomiendan los siguientes criterios para la evaluación de la información por sus propios titulares: acceso y autentificación, confidencialidad, privacidad y disponibilidad; el nivel de protección de la confidencialidad, privacidad y disponibilidad dependerá de la naturaleza de la información (datos). Las organizaciones que trabajan con información sanitaria personal deben clasificar dichos datos como confidenciales.

Hoy se hace necesario definir una cultura común de protección de datos y mejores prácticas; utilizar estándares que garanticen la seguridad y confidencialidad de la información. El potencial de la HCE es inmenso si se piensa en términos de una eficiente gestión del conocimiento: el análisis de la información de pacientes, generada por los profesionales durante el proceso asistencial en un centro médico. La introducción de la HCE urge a reforzar la seguridad de los datos personales de salud para garantizar su privacidad; a pesar de la gran cantidad de medidas de seguridad técnicas y de recomendaciones existentes para el ámbito sanitario, hay un **aumento en las violaciones de la privacidad de los datos personales de los pacientes en centros sanitarios**, en muchos casos como consecuencia de errores o descuidos de los profesionales sanitarios (Sánchez-Henarejos et al., 2014).

En cuanto a las políticas de acceso a los sistemas de HCEs, se discute si deben ser las personas o las entidades quienes concedan los permisos en las historias clínicas electrónicas; mientras los entornos inalámbricos han sido todavía poco estudiados, y la formación técnica de los usuarios es otro aspecto a tener en cuenta. En general parece que “el control de acceso es gestionado por usuarios y profesionales médicos en la mayoría de los sistemas, lo que promulga el derecho del paciente a controlar su información” (Senor, Alemán y Tovar, 2012).

La confianza de los pacientes es frecuentemente considerada como un claro obstáculo para el desarrollo de la HCE en particular y la sanidad electrónica en general, así lo estima Rauer (2012), quién piensa que la confianza en el personal sanitario puede sufrir si los pacientes no creen en la manera en que sus datos médicos son almacenados[204].

Internet ofrece múltiples oportunidades para la gestión de enfermedades, a través de páginas web de información *(Health 1.0)* y aplicaciones interactivas como consultas electrónicas, foros...y registros médicos electrónicos *(Health 2.0).* Sin embargo, se requieren algunas habilidades o conocimientos para que cada individuo pueda beneficiarse de estas aplicaciones, se trata básicamente de conocimientos sobre herramientas de sanidad digital, según señalan Van der Vaart, Drossaert, De Heus, Taal y Van de Laar (2013). Su estudio sobre pacientes con enfermedades reumáticas y los tipos de problemas que encuentran cuando acuden a Internet en relación con su enfermedad, revela que entre los problemas a los que se enfrentan los usuarios está la protección y el respeto a la privacidad. El estudio concluye que muchos pacientes tienen insuficientes conocimientos para usar adecuadamente *Health 1.0 y Health 2.0*, desde la formulación de búsquedas a la evaluación de la información identificada; así, los profesionales sanitarios deben concienciarse de la falta de conocimientos sobre herramientas de *eHealth* por parte de los pacientes.

Estamos generando cada vez más datos sobre la salud de las personas, procedentes de un mayor número de fuentes, como nunca antes, incluidos los registros médicos, notas hospitalarias, pruebas de laboratorio, ensayos clínicos, dispositivos de monitorización y aplicaciones de salud. Los avances en tecnología de la información y en la analítica de datos hacen que sea cada vez más fácil, más económico y más valioso recoger, transferir, vincular, almacenar y analizar estos datos. Este contexto actual ofrece oportunidades casi ilimitadas para generar nuevos conocimientos, mejorar la práctica médica, aumentar la eficiencia del servicio e impulsar la innovación; el informe del *Nuffield Council on Bioethics*[205] examina la ética del uso de datos considerando la relación entre la privacidad y el interés público, y cómo los avances en analítica de datos e informática han sometido a presión a los enfoques más convencionales de la gobernanza de la información, incluido el enfoque para la obtención del consentimiento y la anonimización de los datos para su uso en la investigación médica. Hay que tomar más medidas para garantizar el respeto de los participantes y la protección de sus datos, mediante la rendición de cuentas, respaldada por una buena gobernanza y sanciones penales por el uso indebido de datos. Marginar a las personas que proporcionan datos significa arriesgar la confianza de las generaciones actuales y futuras, exponer a las personas a riesgos inaceptables y, en última instancia, perder los beneficios de la investigación. El *Nuffield Council on Bioethics* establece en su informe los principios éticos fundamentales para el diseño y la gobernanza de las

[204] El estudio de Rauer U en Alemania concluye que para ganar la confianza de los pacientes, el operador de sanidad electrónica debe idealmente tener naturaleza médica, y permitir que los pacientes se involucren en el tratamiento de sus datos.

[205] Informe "El almacenamiento, vinculación y uso de los datos en la investigación biomédica y la atención de la salud: cuestiones éticas" de 2015.

iniciativas para el tratamiento y el uso de los datos, e identifica ejemplos de buenas prácticas relevantes para cualquier profesional que vaya a intervenir en una iniciativa que trate con datos.

Auffray et al. (2016) en sus conclusiones y perspectivas futuras defienden las ventajas de la **revolución digital en marcha;** partiendo de una serie de industrias cuyas actividades se han transformado o se han convertido en inoperantes, nos encontramos con nuevos motores de la innovación como son la miniaturización, la automatización, y últimamente cada día con más fuerza la convergencia de la inteligencia artificial, el aprendizaje profundo, y la robótica. En este sentido entienden que la salud no escapará a estos desarrollos; de hecho, ven los grandes volúmenes de datos o Big Data como una fuerza impulsora que desempeñará un papel importante incluso más relevante que en la mayoría de las industrias. En la UE creen que el trabajo transfronterizo es la única manera de superar los retos de esta revolución científica, tecnológica e industrial; el factor más importante es la fuerza de trabajo y los países que lideran el conocimiento de las TIC, que tienen una comprensión de las diferencias culturales y la capacidad y voluntad de trabajar juntos, tienen la mejor oportunidad de alcanzar el éxito.

Los profesionales sanitarios son administradores de la información personal de los pacientes, y tienen el deber profesional de salvaguardar dicha información mediante el uso adecuado de la tecnología, insisten Crotty y Mostaghini (2014), que defienden la posición de estar alerta frente a la tecnología y los sistemas que se utilizan, a la vez que recomiendan tomar precauciones para prevenir la filtración de información del paciente; creen que **a medida que la cantidad y el uso de la información digital van en aumento, también crece el riesgo de un acceso indebido a datos de carácter personal.** Estos investigadores recomiendan a los profesionales sanitarios, para estar mejor capacitados y proteger la información, que sean conscientes de los conceptos básicos que implican mantener los datos seguros, lo que comprende el cifrado de los dispositivos, la comprensión de las políticas y regulaciones locales.

3.4.5. Transferencia internacional de datos.

La privacidad y la protección de datos son considerados un tema controvertido especialmente en cuanto a la cooperación internacional. Las actuales políticas de seguridad interna de la UE, así como el creciente flujo de datos, incluido el intercambio de datos de carácter personal entre agencias y actores varios a nivel europeo en las áreas de libertad, seguridad y justicia (Europol, Eurojust, OLAF), y el acceso de agencias de la UE a datos almacenados en sistemas de información europeos como SIS (II), VIS, CIS o Eurodac, llevan a plantearse algunas preguntas sobre el equilibrio entre los derechos individuales y la seguridad; Franziska (2011).

La verdadera armonización debe atender a la transferencia internacional de datos (fuera del espacio de la UE) en general, y de salud en particular; hoy en día cualquier comunicación de datos en el Espacio Europeo constituye una **cesión de datos** a efectos de la aplicación de la LOPD[206]. En el caso de una transferencia internacional de datos, ésta queda sujeta a aplicación de las disposiciones contenidas en la LOPD y en su Reglamento. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en las citadas normas, será necesaria la autorización del Director de la AEPD, salvo que: (a) los datos se transfieran a un país que ofrezca un nivel adecuado de protección o (b) se trate de supuestos legalmente excluidos de la autorización del Director. El título V de la LOPD trata sobre las transferencias internacionales, un punto muy interesante, aunque hace escasa referencia explícita a los datos de salud. Como norma general en su artículo 33 establece:

"1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

Así, una importante garantía del Derecho Comunitario en cuanto a la transferencia internacional de datos es la **necesidad de que los receptores de los datos cumplan con las normas básicas de la UE sobre protección de datos.**

Actualmente son considerados países con un nivel de protección similar al que otorga la LOPD todos los Estados miembros de la UE, incluyendo todos los miembros del Espacio Económico Europeo, y los Estados que la Comisión Europea ha declarado que garantizan un nivel de protección adecuado[207]. Respecto a los **EE.UU. (sin perjuicio del hecho de seguir siendo considerado un país que no ofrece,**

[206] La Instrucción 1/2000 de 1 de diciembre, de la Agencia Española de Protección de Datos, define la transferencia internacional de datos como: "toda transmisión de datos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero".

[207] Suiza, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Noruega, Islandia, Liechtenstein, Israel y Uruguay y Nueva Zelanda.

según la normativa comunitaria, un nivel de protección equiparable o adecuado), se reconocía hasta el año 2015 el nivel adecuado a las entidades estadounidenses adheridas a los principios de "Puerto Seguro"; a partir del caso Schrems, se sustituyó el "Puerto Seguro" por el "Escudo de Privacidad" (Gómez Múñoz y Cañabate Pérez, 2016; Weiss y Archick, 2016). En cuanto a Canadá solamente respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, y los datos de carácter personal incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los EE.UU.

Por lo tanto, los países de la UE no consentirán el envío de datos a los EE.UU. (si no es bajo el acuerdo del "Escudo de Privacidad"), y sólo lo harán a países que adopten el marco regulatorio europeo. Así, distintos países latinoamericanos parecen empezar a implantar el modelo europeo de protección de datos (ver apartado 4.4.), también por motivaciones comerciales (para **poder acoger centros de datos**[208] que pueden convertirse en la fuente de un negocio muy lucrativo). Todo ello tiene un impacto claro sobre las compañías de EE.UU. que operan en esta zona geográfica. Cabe entonces preguntarse si se impondrá la normativa europea como modelo de una futura política internacional de privacidad.

Respecto a la investigación basada en biobancos, en los EE.UU. la privacidad está protegida principalmente por la *Privacy Rul*e de la Ley de Portabilidad y Responsabilidad del Seguro de Salud y la *Common Rule* Política Federal para la Protección de los Sujetos Humanos[209], aunque ninguna de las normas fue creada para funcionar específicamente en el contexto de la investigación con biobancos, por lo que no se aplica a todas las investigaciones basadas en biobancos (Harrel y Rothstein, 2016). No sólo es difícil determinar cuándo se aplica la *Privacy Rule* de HIPAA o la *Common Rule*, sino que estas leyes aplican diferentes estándares para la protección de la privacidad. Por otro lado, existen muchas otras leyes federales y estatales que pueden ser aplicables a un biobanco concreto, a un investigador o a un proyecto particular. La legislación de EE.UU. no aborda directamente el intercambio internacional de datos o muestras fuera del acuerdo con la UE (el mencionado "Escudo de Privacidad") hasta la fecha.

La armonización de las normas de privacidad es una instrumento que contribuye al desarrollo de la investigación internacional (como defienden Rothstein y Knoppers, 2016); aunque las leyes de privacidad en algunas jurisdicciones pueden no prohibir las colaboraciones internacionales, un enfoque de la privacidad diferente en cada jurisdicción puede complicar el intercambio internacional de datos, por lo que conviene describir un marco común para el proceso de armonización de las leyes de privacidad (Rothstein, Knoppers y Harrell, 2016), tan necesario en la investigación con biobancos.

[208] Se trataría de considerar a América Latina como un potencial concentrador de datos; que se piense en América Latina como una opción para el establecimiento de centros de datos, al tratarse de una región en la que se respetan principios internacionalmente aceptados de protección de datos, como señala Franco, 2016.

[209] *Federal Policy for Protection of Human Subjects.*

Capítulo 4. Ventajas, influencias y barreras a la covergencia.

En este capítulo se abordan las ventajas y los obstáculos a la convergencia con el modelo de la UE, así como la influencia internacional del modelo europeo de protección de datos de carácter personal, a partir de este derecho fundamental nacido en Europa, donde el dato de salud recibe protección especial. Se atiende especialmente a la experiencia en América Latina, donde se ha proyectado este derecho en las últimas décadas, a través de los fuertes lazos de cooperación forjados durante años, incluidos los vínculos lingüísticos, culturales y legislativos. Finaliza el capítulo abordando brevemente el nuevo RGPD (que merece desde luego se tratado debidamente en futuras investigaciones), para destacar su trascendencia e implicaciones en la futura protección de los datos de carácter personal, tanto para particulares como para todas las organizaciones que operan en territorio de la UE.

4.1. Introducción.

El derecho a la protección de los datos de carácter personal algunos investigadores lo valoran "como un derecho humano de tercera generación, consagrado y garantizado entre los derechos fundamentales" de las constituciones de América y Europa (Saltor, 2013); el derecho a la protección de los datos de carácter personal, sería considerado una especie autónoma del género derecho a la intimidad, que "procura el respeto por la dignidad de las personas, buscando generar las condiciones necesarias para el desarrollo integral de la personalidad en el contexto de nuestra sociedad tecnológicamente desarrollada".

Esta tesis doctoral surge de la idea de analizar el derecho a la protección de datos personales, nacido en Europa y proyectado en las últimas décadas en otras zonas geográficas como Latinoamérica, como reivindican García y de los Ángeles (2013); tanto en Méjico como en otros países de América Latina, España ha sido un país que ha tenido gran influencia debido a los fuertes lazos de cooperación forjados a lo largo de la historia, incluido el lingüístico y cultural. El ámbito de desarrollo legislativo no ha sido la excepción[210], y no sorprende que a partir de la LORTAD y de la actual LOPD, el desarrollo de la normativa relativa al derecho de protección de datos personales haya evolucionado con repercusiones al otro lado del Atlántico, con el surgimiento de legislaciones similares en países como Argentina, Colombia, Costa Rica, Perú y Méjico. Méjico, como muchos otros países latinoamericanos, presenta un desfase de casi 20 años, respecto a España, si nos remontamos a la publicación de la primera normativa española de protección de datos personales de 1992 (LORTAD), y la LOPD de 1999; hasta la Ley mejicana de 2010. Este contexto

[210] La Red Iberoamericana de Protección de Datos (RIPD) se creó a partir del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD), con asistencia de representantes de 14 países iberoamericanos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003. Esta Red tuvo su reflejo en el Reglamento aprobado a raíz del VI Encuentro, celebrado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008, que supuso la consolidación regional al fijarse sus objetivos y formalizarse su régimen interno. La Red tiene como finalidad promover los desarrollos legislativos necesarios para que se garantice una regulación avanzada del derecho a la protección de datos de carácter personal en un entorno democrático, teniendo presente la necesidad del continuo flujo de datos entre naciones que poseen lazos en común.

lleva a entender que el país sea vulnerable, ya que Méjico está no sólo en un proceso de implementación y adecuación de la normativa, sino de algo más importante si cabe, de sensibilización de la ciudadanía; esta vulnerabilidad también hace referencia a la ausencia de una adecuada delimitación judicial y jurisprudencial del derecho, algo que resulta lógico por otro lado debido a la reciente incorporación a su ordenamiento jurídico**.**

Así pues, la protección de datos (o el respeto a la privacidad), ha ido extendiendo fuera del ámbito geográfico europeo en las últimas décadas, y existen nuevos procesos normativos en desarrollo en distintos otros países de Latinoamérica como se acaba de detallar; cada día es mayor la regulación, con más amplia cobertura en textos legales, incluyendo en algun caso la aprobación de reformas constitucionales, como ha sucedido en México[211] [212], quedando aún hoy espacio para el desarrollo pues no todos los países disponen de una normativa específica. Conviene aquí citar la Ley 25.326 de protección de datos de Argentina; o la Ley 18.331, de agosto de 2008, de protección de datos de Uruguay, la Ley 29733/2011, de protección de datos de Perú; la Ley 8968/2011, de protección de la persona frente al tratamiento de sus datos personales, de Costa Rica; la Ley 787/2012, de protección de datos personales, de Nicaragüa; Ley 1581/2012, estatutaria de protección de derechos personales, de Colombia. A la vez se van produciéndo avances a destacar en algunas otras zonas geopolíticas (China, Kenia o Burkina Faso), lo cuál abre la puerta a un futuro sobre crecimiento de la protección y posible convergencia internacional, hoy más una expresión de deseo que una realidad.

Es importante atender al principio de consentimiento, donde normalmente se distinguen dos tipos: uno expreso y otro tácito; este último, en Méjico (a diferencia de otros países de la zona) consiste en que se otorga "cuando habiéndose puesto a su disposición el aviso de privacidad, el titular no manifiesta su oposición. El consentimiento tácito será válido como regla general, salvo que la Ley exija el consentimiento expreso (artículos 13 y 14 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares)"[213].

[211] Como recuerda Mañas (2009) el 12 de diciembre de 2008 se aprobó la adición de un nuevo párrafo al artículo 16 de la Constitución al objeto de reconocer de forma expresa y como derecho fundamental el derecho a la protección de datos).

[212] "El derecho a la protección de datos personales en México aparece por primera vez en el año 2002 en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Después, con las reformas constitucionales de 2009, de los artículos 16 y 73. Evolución legislativa que concluye, recientemente, con la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), y de su Reglamento (2011). Este primer surgimiento fue poco eficaz, ya que entonces, solamente se refería en la Ley de Transparencia la protección de datos personales en posesión de la administración pública y no aquellos en posesión de particulares, como ocurre actualmente" (García Guzmán, 2013).

[213] Como recuerdan García Guzman (2013), añadiendo una útil observación de cara a la homeneización: "De igual modo, que existen certificaciones internacionales en este ámbito, es importante crear un mecanismo similar de validez a nivel nacional, regulado por el Instituto y cuya licencia se otorgue a profesionales técnico-especializados en la materia. Lo anterior, conducirá a paso firme hacia la urgente homogenización de procesos en protección de datos. En consecuencia, se promovería el interés de la comunidad jurídica en esta área para lograr avances significativos en el cumplimiento de la LPDP, además se incentivaría la cooperación y participación internacional en este campo".

En cuanto a la diferencia de normativas en países que han seguido el modelo de la UE, conviene destacar algunas relativas a la legislación mejicana (recogidas por García Guzmán):

-La Ley en Méjico (si es comparada con la española) no contempla el registro de ficheros ante la autoridad reguladora.

-El ámbito de sanciones en la legislación mejicana (artículos 64 a 66 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares) es más gravoso que el español, pero con la importante nota que hace la Ley para modular la capacidad sancionadora en función de la "capacidad económica del responsable", algo que debe definir la propia autoridad competente.

En cuanto a las similitudes, tanto ambas legislaciones (mejicana y española) adaptan prácticamente la misma posición respecto al derecho de cancelación, puesto que como bien apunta Mendoza (2013), señalan como finalidad última del derecho de cancelación la supresión del dato, lo que quiere decir "la destrucción mediante el borrado, pero antes de ello el efecto que tiene la cancelación es el bloqueo previo de la información por un tiempo determinado, para efectos de posibles responsabilidades futuras surgidas de las relaciones contractuales que tuviera el titular de la información"; el plazo de bloqueo vendrá determinado por la legislación aplicable a cada caso.

En el caso de la República Argentina, su Constitución incorporó en la reforma de 1994 una nueva garantía con el fin de proteger los datos personales, para que después, a finales del año 2000, entrara en vigor la Ley No. 25.326 (de protección de datos personales), que recoge la garantía constitucional de habeas data (que fue incorporada en el artículo 43, tercer párrafo, de la Constitución)[214]. Esta norma de protección de datos estipula la creación de un órgano de control (es el equivalente a una agencia de protección de datos personales, llamado Dirección Nacional de Protección de Datos Personales), que está dirigido por un funcionario dependiente del Ejecutivo (Ministerio de Justicia) y dispone de pocos recursos, lo que dificulta su efectividad, a pesar de disponer de un nivel de protección adecuado de acuerdo con la Comisión Europea. **Argentina es el país pionero en Latinoamérica en materia de protección de datos personales, que además reconoce el derecho al olvido desde el año 2008**[215].

Saltor afirma que "la ausencia de un órgano de control independiente del Poder Ejecutivo ha frustrado las intenciones y el espíritu de la ley argentina 25.326", a pesar de que el proyecto de ley sancionado por el Congreso de la Nación Argentina había previsto un órgano de control dotado de

[214] Como recoge Saltor (2013).

[215] Protección de datos en Argentina. Recuperado de http://www.novagob.org/pages/view/207197/proteccion-de-datos-personales-en-argentina. Último acceso 4 Deciembre 2016.

autonomía funcional[216]; con el veto del Presidente De la Rúa, la Dirección Nacional de Protección de datos quedó debilitada y en situación de dependencia del gobierno de turno.

El **modelo europeo en cambio ha dotado de independencia a las autoridades de control** para así facilitar la eficacia a la legislación de protección de los datos de carácter personal; en España por ejemplo la Ley recoge el carácter independiente del órgano de control y de su Director, con un tiempo fijo de mandato garantizado que sólo se puede reducir de acuerdo a un número específico causas (graves) de cese; como recoge la AEPD: "La Directora puede cesar por expiración del mandato, renuncia, fallecimiento o separación acordada por el Gobierno en caso de: incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por un delito doloso. La Directora no puede recibir instrucciones de ningún poder o autoridad y actúa con pleno sometimiento al Derecho. Ejerce sus funciones con dedicación exclusiva, plena independencia y total objetividad"[217].

4.2. Análisis y comparación de las seis mayores economías de la UE y Latinoamérica.

Cuando se trata de protección al consumidor, la Declaración Presidencial de la Cumbre de las Américas de 1998 y otra serie de conferencias Internacionales celebradas desde entonces (Declaración de Florianópolis con los representantes de países de América Latina y Caribe; Comunicación de Brasilia con los Presidentes de países de América del Sur; Declaración de Rio de Janeiro de la Reunión Intergubernamental de TIC para el Desarrollo; Declaración del Grupo de Río; Declaración de Santiago del Grupo de Rio; Encuentro de Ministros de la UE) dejaron bien patente que todos los países de América se comprometen a mejorar el acceso y la prestación de servicios orientados a la salud a través de las TIC. Pero se trata de analizar en este contexto, qué grado de protección reciben los datos de carácter personal.

En general la UE ha tratado de garantizar a los consumidores un mayor grado de protección; el paciente tiene el derecho a prohibir la cesión de datos de salud (Smith, 2011) y los receptores extranjeros de historiales medicos electronicos (EHRs) deben cumplir con las normas básicas de protección de datos de la UE (Hiller, McMullen, Chumney, y Baumer, 2011); la protección que ofrece la normativa de EE.UU. va en aumento, pero es limitada si la comparamos con la UE, puesto que los pacientes no tienen control sobre la recogida inicial de información sensible, de salud, y tiene poco control sobre la información que puede ser compartida posteriormente con otras entidades sanitarias o aseguradoras. Los países latinoamericanos en

[216] Posteriormente el Ejecutivo (a través del Decreto 995/2000) vetó los incisos 2o y 3o del artículo 29 de la ley, suprimiendo cualquier atisbo de independencia del órgano de control. El vetado inciso 3o del artículo 29 hacía referencia al nombramiento de un Director seleccionado entre profesionales con antecedentes en la materia y designado por un plazo de cuatro años por el Poder Ejecutivo Nacional, con acuerdo del Senado de la Nación.

[217] AEPD. Funciones de carácter general. Recuperado de https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/el-director-ides-idphp.php. Último acceso 5 diciembre 2016.

general se definen por una ley aplicable débil, y la falta de autoridades de protección de datos a la hora de aplicar la ley, pero aquellos países que deseen participar en el tratamiento de datos con Estados miembros de la UE, deberán ofrecer un nivel adecuado de protección (Birnhack, 2008). Bates (1997) aborda el riesgo que supone la creciente digitalización para la confidencialidad de los datos personales; el riesgo crece a la vez que las compañías del sector sanitario recogen y tratan información sensible de los pacientes conectados en red. De acuerdo con Del Villar, de Leon y Hubert (2001) las bases de datos son especialmente relevantes cuando se trata de información sobre el crédito al consumo: un consumidor se siente más obligado a pagar sus deudas cuando es consciente de que de no hacerlo su nombre sera registrado en una base de datos que puede ser utilizada por distintos acreedores y empresas de servicios.

En esta investigación he analizado la ley aplicable, definición de datos personal, dato personal sensible y herramientas de aplicación de la ley (ver tablas 4.0. y 4.1.).

Tabla 4.0.
Ley de protección de datos por país (Latinoamérica)

País	Ley Aplicable	Definición de Dato Personal Sensible	Aplicación de la Ley/Sanciones
Brasil	Brasil no dispone de una norma específica de protección de datos. Pero existen principios generales y provisiones sobre protección de datos y privacidad en la Constitución Federal, en el Código Civil y en otras leyes; de acuerdo con la Ley de Internet cada usuario es considerado un "consumidor" a los efectos de la protección del consumidor.	No existe definición legal de 'dato sensible' o equivalente.	No existe autoridad de protección de datos, así la aplicación de la ley es a través de procedimientos administrativos, demandas civiles individuales o demandas de grupo, que pueden iniciarse por el sujeto, por las autoridades (Abogado del Estado, Oficina de Protección del Consumidor y/o el Regulator sectorial) o por una asociación de defensa de intereses colectivos.
Méjico	La Ley Federal de Protección de Datos Personales en Posesión de los Particulares se aprobó el 5 de julio de 2010 y entró en vigor el 6 de julio de 2010. La Ley sólo se refiere a particulares o entidades legales que procesan datos personales, y no al gobierno, entidades de reporte de créditos que se rigen por su propia ley, ni a personas que recojan o almacenen datos personales con fines particulares y sin el propósito de revelarlos ni de hacer uso comercial de los mismos.	'Dato personal Sensible' es todo dato que se refiera a las áreas más íntimas de la vida del sujeto, cuyo mal uso puede llevar a la discriminación o serio riesgo para el sujeto. La definición incluye datos que pueden revelar: origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filisóficas o morales, afiliación sindical, ideas políticas, y orientación sexual.	La Ley es de orden público y de aplicación en toda la República. Tiene como propósito la protección de los datos personales en posesión de particulares, para exigir el procesamiento legítimo, controlado e informado, y asegurar la privacidad y el derecho al control de la información personal, las infracciones a la Ley pueden acarrear sanciones pecuniarias o prisión.
Argentina	La sección 43 de la Constitución Federal garantiza a los ciudadanos acción judicial expeditiva para acceder a la información personal contenida en bases de datos públicas y	Información o dato sensible significa 'información personal que revele origen racial o étnico, ideas políticas, creencias religiosas, posiciones filosóficas o morales, afiliación sindical, o cualquier información	La DNPDP es responsable de la aplicación de la protección de datos. Bien actuando de oficio o a instancia del perjudicado, el defensor del pueblo o asociaciones de consumidores, el DNPDP está autorizado para

	privadas y para reclamar su rectificación, actualización, confidencialidad, o supresión en caso de error. La Ley No. 25326 (PDPL), que entró en vigor en octubre de 2000, ofrece una más amplia protección de los datos personales siguiendo de cerca la ley española. El 30 de junio de 2003 la Comisión Europea reconoció que Argentina ofrece una nivel adecuado de protección.	referida a la salud o a la vida sexual'.	comenzar una investigación cuando sospeche que el PDPL se haya infringido. Las sanciones administrativas incluyen avisos, suspensión del derecho a mantener una base de datos, la imposición de sanciones pecuniarias, o la cancelación de la base de datos.
Colombia	El artículo 15 de la Constitución colombiana establece derechos fundamentales a la intimidad, la imagen, y protección de datos. La Ley 1581 de 2012 ('Ley 1581'), revisada por el Tribunal Constitucional de Colombia, con la Decisión C-748/11, contiene regulaciones completas sobre protección de datos, incluyendo el derecho constitucional a saber, actualizar y rectificar información en bases de datos o archivos. La Ley se refiere a datos personales almacenados en cualquier base de datos o archivo público o privado: el titular del dato (sujeto) siempre debe dar consentimiento, previos, informado y expreso. El Decreto 1377 de 2013 es la segunda regulación en materia de protección de datos, que incluye el derecho al consentimiento, el procesamiento, el tratamiento de datos sensibles y la transferencia internacional.	Bajo la Ley 1581 y el artículo 3 del Decreto 1377 ´datos sensibles´ son datos que se refieren a la intimidad del titular de los datos, o que, si revelados sin consentimiento, pudieran llevar a la discriminación, como datos referidos al origen racial o étnico, orientación política, creencias religiosas o filosóficas, afiliación sindical, a asociaciones sociales, de derechos humanos, y datos relativos a la salud, a la vida sexual y biométrica.	La superintendencia de Industria y Comercio puede iniciar investigaciones administrativas contra aquellos que infringen las provisiones de la ley, asó como imponer multas y sanciones que incluyan el cierre temporal o permanente de las actividades del sujeto que infringió el régimen de protección de datos. La penalización según la Ley 1581 sólo se aplica a entidades privadas. Si la ofensa se comete por parte de una entidad pública, la Superintendencia de Industria y Comercio se dirigirá a la oficina del Fiscal General para iniciar la investigación. Los titulares de los datos tienen derecho a iniciar, ante un juez colombiano, una acción constitucional.
Venezuela	No dispone de ninguna regulación sobre protección de datos pero hay principios generales establecidos en la constitución de la República Bolivariana de Venezuela y desarrollado por decisiones del Tribunal Supremo. Estos principios son el marco para la protección de datos, pues su propósito es salvaguardar el honor, la vida privada, la intimidad, la propia imagen, la confidencialidad y la reputación de los ciudadanos.	No existe definición legal de ´dato personal' en ninguna ley .	No existe autoridad de protección de datos en Venezuela. La aplicación puede producirse a través de procedimientos administrativos o penales, demandas civiles individuales y acciones colectivas, iniciadas por los individuos o autoridades públicas.
Chile	La protección de datos personales se aborda en distintas leyes específicas, y en estipulaciones repartidas en leyes relacionadas o complementarias e incluye una acción de protección constitucional. La Ley 19,628 'sobre la protección de la vida privada', comúnmente llamada	Bajo la PDPL, los datos personales sensibles se refieren a las características físicas y morales de la persona, o a los hechos y circunstancias de su vida privada o vida íntima, como costumbres personales, origen racial, ideologías y opiniones políticas, credo o creencias religiosas, estado de salud físico y mental, y la vida sexual.	Cada titular del derecho tiene el derecho de acceso a sus datos, y puede solicitar retirada o cancelación. Pero peticiones para rectificación de la información puede ser denegada en ciertos casos. El titular puede iniciar una queja ante el Juez de Letras local o el juez civil local y puede solicitar daños patrimoniales y morales, incluyendo sanciones pecuniarias.

	'Ley de Protección de Datos Personales' (PDPL), define y se refiere principalmente el tratamiento de información personal en bases de datos públicas y privadas. La última modificación es del 17 de febrero de 2012.		

Fuente: tabla de elaboración propia a partir de datos del manual de protección de datos, DLA Piper, 2016.

La Directiva de la UE de protección de datos data de 1995 pero los enormes cambios tecnológicos han obligado a aprobar una nueva regulación, que será directamente aplicable en cada Estado miembro. Los terminos “regulación” y “directiva” son usados de forma prácticamente equivalente, pero la Directiva de 1995 ha sido desarrollada y aplicada por cada Estado miembro con distintas leyes en cada país como se puede comprobar en la tabla inferior (referida a las seis mayores economias de la UE de acuerdo al PIB).

Tabla 4.1.
Ley de protección de datos por país (UE).

Pais	Ley Aplicable	Definición de Dato Personal Sensible	Aplicación de la Ley/Sanciones
Alemania	La "Bundesdatenschutzgesetz" (BDSG) tiene por objetivo proteger datos personales recogidos por autoridades públicas federales y empresas privadas. Cada *Land* alemán tiene una ley de protección de datos independiente que protege los datos personales del tratamiento y uso por parte de las autoridades públicas de cada uno de los 16 *Länder*.	Origen racial o étnico, opiniones políticas, religiosas o creencias filosóficas, pertenencia sindical, salud o vida sexual.	Las infracciones de la lay están sujetas a multas pecuniarias hasta de €300.000. Si existe dolo o si existe beneficio económico (delito) la pena será hasta de 2 años de cárcel. Las autoridades también tienen potestad para retirar las ganancias generadas por el incumplimiento de la ley.
Reino Unido	El "Data Protection Act 1998" entró en vigor en el año 2000. La aplicación de la ley corresponde al "ICO" (Information Commissioner's Office").	Origen racial o étnico, opiniones políticas, creencias religiosas o de semejante naturaleza, pertenencia sindical, salud o condición física o mental, vida sexual.	Multas hasta £500.000 por graves violaciones de la ley. Las firmas de servicios financieros se rigen por el Financial Conduct Authority cuyos poderes sancionadores incluyes multas ilimitadas.
Francia	La Ley no. 78 17 del 6 de enero de 1978 conocida como 'Informatique et Libertés', fue modificada por la Ley no. 2004-801 del 6 agosto 2004, en aplicación de la Directiva 95/46/CE. La aplicación de la ley corresponde a la 'Commission Nationale de l´informatique et des Libertés' ('CNIL').	Orígenes raciales y étnicos, opiniones políticas, filosóficas o religiosas, afiliación sindical, o datos concernientes a la salud y a la vida sexual.	La CNIL tiene el poder de proceder a realizar verificaciones e imponer sanciones hasta €150.000 por la primera infracción, en caso de una segunda en los siguientes 5 años hasta €300.000, y/o exigir el cese del tratamiento de datos,, o incluso €1.5M para personas jurídicas, y/o sanciones de distinta índole.
Italia	El decreto legislativo no. 196 del 30 de junio de 2003 ("Codice in materia di protezione dei dati personali") traspone las Directivas 95/46/CE, 2002/58/CE y 2009/12/CE.	Origen racial o étnico, religioso, filosófico u otras creencias, opiniones politicas, afiliación a partidos politicos y sindicatos, asociaciones, organizaciones de carácter religioso, politico, filosófico o sindical, la salud o el sexo.	The "Garante" tiene capacidad para nombrar expertos, proceder a realizar inspecciones, requerir documentación y acceso necesarios. Las sanciones incluyen multas de €50.000 a €300.000.
España	La LOPD de 1999 es una versión actualizada de la LORTAD de 1992. La aplicación de la ley se realiza a través de la Agencia Española de Protección de Datos (AEPD); la última reforma tuvo lugar en 2011.	Orientación política, religión, creencias, afiliación sindical, orígen étnico, salud y vida sexual. Cada categoría de información sensible disfruta de una grado diferente de protección.	Sanciones principalmente pecuniarias, desde €900 a €40.000 para infracciones leves, a €40.001 hasta €300.000 para las graves, y desde €300.001 a €600.000 para las más graves.
Holanda	La ley holandesa del año 2000 "Wet Bescherming Persoonsgegevens" (WBP) aborda el tratamiento de los datos personales, siguiendo la Directiva de 1995. La aplicación de la ley se realiza a través de la Autoridad Holandesa de Protección de Datos ('Autoriteit Persoonsgegevens').	La religión de una persona, o su filosofía de vida, raza, ideas políticas, salud, y vida sexual, afiliación sindical o conducta criminal, así como datos personales referidos a una conducta ilícita o reprobable.	La "Autoriteit Persoonsgegevens" puede imponer las siguientes sanciones: (1) orden administrativa (2) sanciones administrativas hasta un máximo de €820.000 o el 10% de la facturación anual del ejercicio anterior.

Fuente: tabla de elaboración propia a partir de datos del manual de protección de datos, DLA Piper, 2016.

4.3. Revisión de las ventajas para terceros de la convergencia con el modelo de protección de datos de la UE.

Las leyes de protección de datos personales (y el derecho de acceso a la información) están ligadas con derechos individuales, pero los beneficios de la protección de datos van más allá de los consumidores (Del Villar, de Leon y Hubert, 2001); un sistema que protege los datos de forma efectiva genera confianza (tanto por parte de los consumidores como de las compañías) respecto a un tratamiento adecuado y correcto de los datos personales, lo que contribuye al crecimiento de las bases de datos y a la circulación fluída de información para beneficio de consumidores, compañías, y de la economía en general; así, por ejemplo, si los consumidores cumplen con sus obligaciones crediticias y fiscales, el sistema financiero se hará más fiable y seguro, inspirando confianza. Para aquellas compañías en Latinoamérica que deseen hacer negocios fuera de su región geográfica, ser consideradas como respetuosas, adaptándose a la normas de la UE, contribuirá a desarrollar su negocio, aumentando la credibilidad entre los consumidores.

Como afirma Manning (2015) las consecuencia financieras y el impacto en la reputación de la compañía puede ser enorme, si se filtran datos; la cuantía de la sanción dependerá de la jurisdicción, pero es importante conocer cómo afecta al negocio, cómo cumplir con la regulación en vigor, y cómo poner en práctica las medidas de protección adecuadas, también para evitar otros costes asociados.

Puede ser más costoso a corto plazo pero adoptar las más altas garantías en protección de datos permitirá que terceros países puedan acoger desde un primer momento modelos de negocio basados en el Big Data, limitando a la vez el uso desmedido que hacen muchas compañías de los datos de los usuarios. Hemos analizado en la tabla 4.2. la aplicación de los derechos de los consumidores, de acuerdo al nivel de fortaleza o debilidad de los sistemas en vigor.

Tabla 4.2.
Regulación y aplicación de la protección de datos por país (Latinoamérica/UE).

País	Fuerte	Robusta	Moderada	Débil
Brasil (1,8)				X
Méjico (1,3)			X	
Argentina (0,5)		X		
Colombia (0,37)			X	
Venezuela (0,206)				X
Chile (0,25)			X	
Alemania (3,874)	X			
Reino Unido (2,950)	X			
Francia (2,834)	X			
Italia (2,148)	X			
España (1,407)	X			
Holanda (0,9)	X			

Fuente: elaboración propia a partir de datos del FMI, 2014. PIB Nominal en millones De USD/Datos del manual protección de datos, DLA Piper, 2016.

Con la excepción de Argentina no existe una autoridad independiente en la región latinoamericana (ver tabla 4.3.). Una garantía de la normativa europea referida a la transferencia de datos es la necesidad de que el receptor de los datos reúna las normas básicas de la UE respecto a la protección de datos. Este derecho fundamental que asiste a los consumidores pretende garantizar un poder de control sobre cualquier tipo de dato de carácter personal, sobre su uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para el derecho afectado (Mok, 2011)[218], y para ello debe recurrir a los organismos correspondientes.

Tabla 4.3.
Autoridad de Protección de Datos y Órgano de Aplicación (Latinoamérica/UE).

	Authoridad independiente de protección de datos	Aplicación del derecho
Brasil	N/A	Tribunal civil según quien sea demandado
Méjico	N/A	Tribunal civil o penal
Argentina	Dirección Nacional de Protección de Datos Personales (PDP)	Tribunal Federal o local según los casos
Colombia	N/A	Tribunal civil
Venezuela	N/A	Tribunal civil o penal
Chile	N/A	Tribunal civil
UE	Órganos nacionales y regionales de control	Autoridad judicial

Fuentes: tabla de elaboración propia a partir de Del Villar, R. et al. (2001)/manual de protección de datos, DLA Piper (2016).

[218] Mok, S.C. (2011), "Privacidad y protección de datos: un análisis de legislación comparada", Diálogos Revista Electrónica, Vol. 11, No. 1.

Parece razonable pensar que los países latinoamericanos seguirán el modelo de la UE por razones comerciales (como, por ejemplo, para acoger centros de datos de ciudadanos europeos en servidores en su territorio, y poder así tratar sus datos); algunas recientes reformas en Méjico van en esta dirección, habiendo ampliado la protección a información personal recogida por la administración pública e instituciones asimiladas (Da Cunha y Teresa, 2011). Esto tiene un impacto directo en compañías con sede en EE.UU. que operan en este región. En los EE.UU. los derechos del individuo referidos a información de salud se consideran "derechos del consumidor", su modelo considera la privacidad como una "*commodity*", una mercancía, dejando su protección en manos del consumidor, mientras el modelo de la UE lidera la defensa de la protección de datos personales (Craig y Ludloff, 2011).

La actual evolución del modelo europeo va acrecentando la distancia con EE.UU. (Martínez, 2014). Al mismo tiempo las compañías están reclamando la creación de bases de datos que les permitan definir el perfil de sus clientes con mayor fiabilidad (Arellano Toledo, 2012). Mientras en EE.UU. se habla del derecho a la privacidad, la UE habla de la protección de datos personales: el Tribunal de Justicia de la UE ha equiparado repetidamente los dos derechos pero el derecho a la protección de datos ofrece a los individuos mayores garantías (y un control más estrecho) sobre un mayor número de datos que el posiblemente más elemental derecho a la privacidad (Lynskey, 2014). Así algunos autores señalan que cuestiones globales como esta requieren soluciones globales, y proponen una red latinoamericana de protección de datos personales (Argüello, 2005).

En la misma Constitución mejicana, a raíz de la reforma de junio del 2011, en su artículo 16, se aborda el *Habeas Data*, es decir el derecho de cualquier ciudadano a proteger sus datos personales y a solicitar acceso, rectificación, cancelación y oposición sobre su información (llamados derechos ARCO), e incluye la protección en casos donde la información vulnere la imagen, el honor y/o la privacidad, o cause un perjuicio. Este Habeas Data ha sido reconocido en otras constituciones de Latinoamérica como Argentina, Colombia, Perú, Brasil, Uruguay, Venezuela y Costa Rica.

4.4. Influencias del modelo europeo.

Existen evidencias, como hemos visto aquí, de la existencia de una declaración del derecho a la protección de los datos personales en toda Europa y en casi toda América (Saltor, 2013) -al margen de otras jurisdicciones alrededor del mundo (Greenleaf, 2014)-, así como la influencia del Convenio 108 del Consejo de Europa (siguiendo las investigaciones de Greenleaf, 2016).

En este sentido, creo que lo más notable de la normativa en América Latina relativa a los datos personales es la influencia significativamente escasa que ha tenido el derecho de EE.UU., pese a ser una región que de un modo directo o indirecto siempre se recibido la influencia del derecho de ese país, a través de distintos vehículos o alternativas de incorporación que se han denominado, de forma generalizada, "tropicalización"[219]. Interesante si lo ponemos en contexto con el concepto de "americanización" defendido por Kagan (2007), respecto a la leyes europeas (abordado en el apartado 3.4.2.).

Y lo que es más relevante por ello, es que la influencia ha venido de Europa, se trata de las influencias de la regulación de la UE en legislaciones de protección de datos (incluidos los datos de salud) de las naciones de América Latina, especialmente de países como Argentina, Chile, Panamá, Brasil y Paraguay (Gregorio, 2004). El caso de México es especialmente emblemático, como defiende Guzmán Rodríguez (2016) -quién afirma que la ley mexicana de datos personales tiene un 80% de genes europeos-, dado que a raíz de su situación geográfica y geopolítica el país ha tenido una legislación de protección de datos personales con influencias de EE.UU., Asia-Pacífico y la UE, pero a pesar de esta triple influencia el derecho europeo es el que más ha pesado en la configuración del derecho mejicano de protección de datos personales.

El análisis de los distintos regímenes fuera de Europa, y en América Latina específicamente, nos indican pues que las directrices europeas han sido las que mayor influencia han tenido fuera de territorio europeo con un amplio margen, a la vez que esta tendencia sigue creciendo, hasta tal punto que parece no existir alternativa actualmente (o resistencia alguna que tenga coherencia y consistencia, al margen de la política liderada por los EE.UU.), representando la UE un papel de liderazgo hacia la globalización de la normativa de protección de datos (Greenleaf, 2012)[220].

---

[219] Guzmán Rodríguez, H. 2016. Datos personales en Latinoamérica: ¿dónde estamos?. Recuperado de http://www.ismsforum.es/ficheros/descargas/segurilatam001blq1456907052.pdf. Último acceso 2 enero 2017.

[220] Su análisis de 33 de las 39 leyes de protección de datos nacionales fuera de Europa muestra que las normas europeas han tenido mucha mayor influencia fuera de Europa de lo que parece y que la influencia continua creciendo.

4.5. Barreras a la convergencia.

En el contexto actual de globalización y concentración, en este apartado se abarcan, las barreras a la convergencia que se han identificado, en el curso de esta investigación, a partir del modelo de América Latina, teniendo en cuenta en todo momento que cada jurisdicción se encuentra en un momento de madurez y desarrollo normativo diferentes.

En el continente americano existe una realidad diferente a la que existente en Europa en materia de protección de datos. América del Norte empezó a legislar en esta materia en la década de 1980, y el resto de países inició después un proceso de introducción de normas de protección de datos personales que va está todavía en construcción; como bien recoge Saltor (2013) Latinoamérica está experimentando una evolución poco homogénea, con inclusión, eso sí, de cláusulas constitucionales en la mayoría de países, protectoras de los datos personales; se trata del llamado habeas data, una acción constitucional directa de garantía (que actúa como una especie de acción de amparo). Se puede decir no existe homogeneidad entre las distintas coberturas nacionales y, a diferencia de la UE, no disponen de forma generalizada de un órgano de aplicación y garantía del derecho a la protección de datos, y en aquellos casos en que existe, éste no goza de autonomía ni independencia del ejecutivo, por lo que no se puede decir que exista una efectiva protección jurídica de este derecho.

Desde esta experiencia latinoamericana he identificado en el curso de la investigación los siguientes obstáculos a la convergencia de terceros países con el modelo europeo, a la hora de desarrollar un marco jurídico armonizado (y que coinciden parcialmente a gran escala con las barreras al desarrollo del eHealth a nivel global detectadas por la OMS[221]):

[221] A saber: costes, limitaciones legales, culturales, del tipo de infraestructuras, políticas, prioridades, ausencia de demanda, normas, conocimiento, experiencia, y otros (OMS. Survey 2009 Figures. recuperado de http://www.who.int/goe/survey/2009/figures/en/index2.html. Último acceso 10 diciembre 2016).

4.5.1. Subdesarrollo institucional.

Gregorio (2004) ya señalaba que instituciones legales débiles conducen a autoridades difícilmente independientes, y normas y leyes ineficaces (Del Villar, De Leon y Hubert, 2001). Al mismo tiempo, en las últimas décadas el bienestar social en América Latina ha estado subordinado a los objetivos de la política económica del Estado en el contexto de la heterogeneidad de sus sistemas, como recoge Navarro Ruvalcaba (2006)[222], que no se han caracterizado por dar prioridad al desarrollo de los derechos de los ciudadanos, incluido el derecho a la salud y a la protección de sus datos.

Como acertadamente señala Cordero (2016) merece especial mención el papel enormemente activo que deben llevar a cabo los poderes públicos; así, por ejemplo, en marcos regulatorios maduros como Europa se garantiza por ley la defensa de los derechos de los consumidores y usuarios a través de procedimientos eficaces (como pretende ser la certificación), la seguridad y los legítimos intereses económicos de dichos colectivos[223].

4.5.2. El lento ritmo de las reformas.

Explica el pobre desarrollo de los mercados de valores en la región, lo que revela el grado de protección del inversor; esta es una de la regiones del mundo con una menor protección del inversor, incluyendo duras expropiaciones, por ello ha experimentado la caída en el número de compañías cotizadas, en serio contraste con otras regiones con mercados emergentes como Asia y Europa del Este. América Latina es actualmente la zona menos activa en el mundo a este nivel respecto al tamaño de sus economías (Chong, 2007).

En mercados emergentes, incluidos América Latina y el Caribe, existen muchos países como ejemplo de malas prácticas de gobierno corporativo y escasa protección al inversor, como reconocen Kawamura y Rinconi (2015), e incluso dentro de cada uno de estos países con una baja calidad media de protección del inversor, puede existir una alta heterogeneidad entre corporaciones, asociado con niveles heterogéneos de transparencia y calidad de la gobernanza.

[222] Las políticas sociales han girado principalmente en torno a la incorporación de grupos vulnerables a los cambios económicos que se han venido desarollando desde la década de 1980. Lo que resalta del caso latinoamericano es una heterogeneidad en sus sistemas de bienestar social, ya que es posible hablar de modelos o regímenes de tipo universal estratificado, como son los casos de Uruguay, Chile, Argentina y Costa Rica; de modelos o regímenes de tipo dual, como los casos de Méjico y Brasil; y de modelos excluyentes, como los casos de los países de Guatemala, El Salvador y Nicaragua.

[223] En España, por ejemplo, en conformidad con el art. 51 de la Constitución Española.

Por otro lado, las devaluaciones de moneda conllevan fugas de capital junto con inseguridad en programas de inversión de compañías y una falta de consolidación de los mercados de capital como fuente de financiación[224]. La falta de seguridad jurídica es una consecuencia de la ausencia de una protección del inversor de calidad. De acuerdo con el estudio de Dixon y Haslan (2015) en la región lationamericana, los acuerdos internacionales de inversión parecen ser más eficaces en un contexto de mayor integración económica. Es decir, que funcionan mejor cuando proporcionan una protección más alta calidad a los inversores y cuándo se combinan con otros acuerdos de integración económica preferenciales, como los acuerdos comerciales; sin una integración económica o comercial parece difícil que se produzca una convergencia con modelos como el europeo que tiene importantes implicaciones transfronterizas.

4.5.3. Bajos ingresos y analfabetismo.

Son síntomas de la pobreza de la región, que desde la decada de los 90 del siglo pasado ha emprendido la reforma de sus sistemas de salud para reducir las desigualdades en el acceso a la salud (Atun at al., 2015) además de la barrera lingüística; de acuerdo con Bates y Wright (2009) en países en desarrollo la principal actividad en *eHealth* se dirige a los profesionales de la salud en inglés; la traducción de aplicaciones de *eHealth* a otros idiomas, locales, dependerá de los niveles de alfabetización. Bates y Wright creen que barreras culturales y sociales son siempre difíciles de superar, a pesar de las numerosas oportunidades que existen hoy para la colaboración transnacional; como señalan hay avances recientes en materia de traducción automática que facilitan la labor, y van eliminando barreras, aunque en la traducción de aplicaciones de *eHealth* hay que atender al interrogante del nivel de alfabetización y los conocimientos informáticos, entre proveedores de servicios sanitarios, y especialmente entre los propios pacientes.

4.5.4. La fractura digital.

Como apuntan Ragnedda y Muschert (2013) se requiere una reducción de la actual fractura en el desarrollo de las TIC en regiones como América Latina. El aumento de la capacidad de la población en general para beneficiarse de tecnologías de la información y comunicación depende de importantes inversiones en educación general y formación en conocimientos tecnológicas. Un problema grave en América Latina y los países del Caribe es que la mayor parte de los contenidos en Internet se dirigen a nativos en inglés; la mayor parte de las páginas de Internet e intercambios se realizan en inglés, se trata por

[224] De acuerdo con Andrei Schleifer un objetivo clave en la agenda de reformas financieras de América Latina debe ser la mejora en la gobernanza corporativa a través de reformas legislativas (Chong, A, 2007).

lo tanto de la barrera de la división digital o escasa penetración de esta tecnología en una amplia población (Mylona, 2008).

4.5.5. Escasa financiación e insuficiente asignación de escasos recursos.

Resulta difícil que las autoridades dispongan de los medios -financieros, humanos y materiales- suficientes, aún siendo necesarios, y que sean confiados por los gobiernos de forma efectiva para sancionar a las compañías que no cumplen con la ley, por lo que se reduce la capacidad necesaria para aplicar las normas[225]. En la mayor parte de los países el sector de la salud recibe escasa financiación, especialmente cuando se trata del desarrollo de soluciones de *eHealth* en América Latina y el Caribe; esta situación ha provocado deficiencias cuantitativas o cualitativas en la prestación de servicios de salud así como un aumento de las brechas en cuidados básicos; puesto que las limitaciones financieras aquejan a estos países, es improbable que la superación de la fractura en el desarrollo del sector de la salud se alcance fácilmente. Por otro lado, países de América Central y del Sur (incluyendo el Caribe con países como Cuba) están experimentando rápidos cambios sociodemográficos y epidemiológicos, y la naturaleza de sus problemas de salud se están trasnformando para pasar de enfermedades infecciosas en muchos casos a otras crónicas, incluyendo el cáncer (Forman y Sierra, 2016), con el consiguiente aumento del coste a corto y largo plazo.

Como acertadamento apunta Saltor (2013), respecto a la nación Argentina, como Estado federal se trata de un territorio muy amplio y profundamente descentralizado, por lo que se hace necesaria la creación de órganos de control locales, que estén especializados en materia de protección de los datos de carácter personal, y es precisamente la falta de presupuesto la razón comúnmente aportada como argumento político para evitar la creación de una autoridad de protección de datos personales. Propone así, como solución alternativa y temporal (mientras se alcanza una solución al tema presupuestario), la posibilidad de dotar de competencias y jurisdicción en esta materia al Defensor del Pueblo.

4.5.6. Falta de sensibilización.

La ausencia de concienciación sobre protección de datos por parte de una mayoría de la población; puede llevar un tiempo antes de que las compañías asuman sus nuevas obligaciones y las implementen en su procesos internos de tratamiento de datos. Supondrá esfuerzos para que los individuos entiendan sus nuevos

[225] Cedric Lautant (15 septiembre 2011).

derechos y para que las autoridades puedan educar a los interesados acerca del alcance de las nuevas normas. Un objetivo crítico en la agenda de reformas en América Latina debe ser la mejora en el gobierno corporativo a través de reformas legales (Chong, 2007).

Se requiere la sensibilización a través de la enseñanza y el aprendizaje de las personas que viven en estos países, pues no deben ignorar el derecho que les asiste para proteger sus datos personales frente a terceros o frente al propio Estado. Como bien apunta Sandor (2013) "los países o Estados cuyos ciudadanos tienen un mayor conocimiento, aprendizaje y apropiación del derecho a la protección de sus datos personales, son aquellos en los cuales se observa un mayor compromiso estatal en la difusión de este derecho, en la información y en el fomento al control de cada persona sobre sus datos personales"; este aspecto está vinculado al funcionamiento del sistema de reclamación judicial y extrajudicial, que debe ser simple, rápido y operativo.

4.5.7. Ausencia de integración.

Y coordinación entre subsectores de salud, instituciones, y otros agentes sociales e interesados -con duplicación de esfuerzos, solapamiento de responsabilidades y despilfarro de recursos- (Vázquez et al., 2009). Todos los países se encuentran en alguna fase de reforma sectorial, un proceso tendente a introducir cambios sustanciales en el sector salud y en las relaciones entre interesados y los papeles que desempeñan, con vista a incrementar la equidad en los beneficios (De Andrade, 2015; Cotlear et al., 2015; Restrepo-Méndez et al., 2015), la eficiencia en la gestión (García Cabrera, Díaz Urteaga, Ávila Chávez y Cuzco Ruiz, 2015), y la efectividad en la satisfacción de las necesidades sanitarias y expectativas de la población, así como la cobertura universal (Atun at al., 2015; Dmytraczenko, Torres y Aten, 2015; Cotlear at al., 2015; Rao, Petrosyan, Araujo y McIntyre, 2014). Todo ello junto con la ausencia de una regulación regional integrada de protección de datos, cuando se trata de transferencia de datos más allá de las fronteras entre países de la misma región, acarreará problemas para las compañías que deseen transferir datos de uno a otro.

4.5.8. Necesidad de profesionales.

Profesionales que conozcan la tecnología de la salud, que sepan trabajar con el Big Data salvaguardando la confidencialidad. Por ello, gran parte del desafío consiste en superar los obstáculos con liderazgo, formación y especialización, entre otros recursos, para apoyar el desarrollo del proceso de integración y uso de las capacidades de la TIC, que comienza en las escuelas (Sunkel y Trucco, 2010)

también en el campo de la salud pública. Se trata de un aspecto vinculado a la brecha digital en América Latina, que se ha concebido en términos de acceso a la tecnología y, desde esta perspectiva la escuela ha sido pensada como un espacio estratégico para poder eliminar las desigualdades de acceso, aunque una segunda brecha digital surje entre aquellos que tienen las habilidades requeridas para beneficiarse del uso de las TIC y aquellos no las tienen, dependiendo del capital social, económico y cultural. Además existe una brecha geográfica cuando los establecimientos educativos ubicados en zonas urbanas tienen mayor acceso a la tecnología que los que se encuentran en zonas rurales, donde muchas veces ni siquiera se cuenta con servicios básicos como la electricidad. Como defiende Vithiatharan (2014) el Big Data puede contribuir a la mejora de la salud pública, o ser de pobre utilidad si los individuos perciben que su derecho de privacidad es vulnerado (pero también será ineficiente si no existe acceso a las TIC).

Estos obstáculos muestran que las organizaciones sanitarias en América Latina y el Caribe, especialmente en el sector público, no se encuentran aún preparadas para adoptar las TIC con garantías, de forma efectiva, aunque han avanzado con las reformas llevadas a cabo en la región desde la década de los años 80 y 90 del siglo pasado (Yavich y Báscolo, 2016; Dmytraczenko y Almeida, 2015; Gragnolati, Lindelow y Couttolenc, 2013; Couttolenc y Dmytraczenko, 2013). El objetivo de alcanzar un entorno competitivo de *eHealth* debería alcanzarse a través de acuerdos nacionales coherentes dirigidos a facilitar el desarrollo de proyectos e infraestructuras, maximizando los beneficios de recursos financieros limitados. Los gobiernos deben centrarse en su papel como sponsors de la investigación científica y tecnológica, superando la fractura digital, promoviendo la cooperación público-privada. Algunos aspectos internacionales de los servicios de *eHealth* constituyen un cuestión crítica y urgente que debe ser abordada por la Organización Mundial del Comercio y por los grupos regionales de comercio; próximas legislaciones deberían garantizar que la tecnología no coarte los derechos de los pacientes respecto a la confidencialidad o seguridad de los registros médicos[226].

4.6. El Reglamento General de Protección de Datos.

La UE continua avanzando en el proceso de consolidación de una normativa, si cabe más homogénea que la actualmente aplicable, puesto que como se ha comprobado aún dista de ser un régimen jurídico único; la propia Comisión Europea presentó en el año 2012 el Proyecto de Reglamento europeo de protección de datos personales, con el objetivo de uniformar la normativa del espacio común europeo (Saltor, 2013), y el pasado 25 de mayo de 2016 culminó ese largo y complejo proceso legislativo, tras cuatro

[226] Rodrigues y Risk (2003).

años de trabajo intenso[227]; la norma que se ha aprobado es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[228], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos. Este RGPD sólo será aplicable a partir del próximo 25 de mayo de 2018, pues en el transcurso del tiempo que resta hasta dicha fecha, cada Estado miembro, empresas en general, y Administraciones públicas, tendrán que realizar las modificaciones y todo tipo de ajustes necesarios para que puedan no sólo garantizar su cumplimiento sino evitar el riesgo de tener que enfrentarse a elevadas sanciones; Mañas, Caro y Gayo (2016) hablan de un nuevo modelo europeo de protección de datos.

Nuevo modelo, o consolidación del modelo europeo con una profunda actualización a partir de la experiencia de 21 años, desde que se aprobó la Directiva 95/46/CE, para hacer frente a los desafíos tecnológicos. Este nuevo marco jurídico viene reforzar los derechos del individuo (el verdadero protagonista y titular de este derecho fundamental -perdón por la insistencia-), y a someter a una mayor responsabilidad ("accountability") a los responsables y encargados del tratamiento. Todo ello pues es bien cierto que los ciudadanos estamos viviendo una veradera revolución tecnológica imparable, con novedosos productos y servicios que nos ofrecen numerosas ventajas indudablemente, como consumidores y usuarios, pero que por otro lado conllevan retos, como evitar fallos en seguridad que pueden afectar a nuestros derechos fundamentales como, y aquí se encuentra incluido el privilegiado derecho a la protección de datos. Es por ello que, como defiende Rincón (2016), "la certificación es un mecanismo de autorregulación o corregulación que pretende solventar todos estos conflictos pero en la actualidad no cuenta con el respaldo e implicación de todas las partes interesadas, incluyendo especialmente a los fabricantes, las organizaciones de consumidores y usuarios y la sociedad en su conjunto". Así, Rincón apunta acertadamente a "dos potentes instrumentos pueden venir a paliar estos déficits en el marco europeo. En primer lugar, el nuevo RGPD que apuesta decididamente en su sección 5 por la **implementación de medidas proactivas** con objeto de proteger los derechos de los usuarios. Estos mecanismos suponen una alternativa al excesivo desarrollo normativo, pues pueden adaptarse eficientemente al potencial desarrollo tecnológico. Asimismo, el 7º Programa Marco de la Comisión Europea también viene fomentando desde 2007 el estudio e **implementación de mecanismos de certificación** sobre la base de los cinco criterios de evaluación del paquete «Legislar mejor» (eficiencia, eficacia, coherencia, pertinencia y valor añadido de la UE)".

El RGPD llega como resultado del reconocimiento en la UE de la existencia de distintas prácticas, poco armonizadas, a consecuencia de la regulación aplicada en su derecho interno por parte de cada Estado miembro, a la vez que las sentencias dictadas por TJUE han modulado el derecho y exigen una armonización

[227] Hoy entra en vigor el reglamento de protección de datos en toda Europa. Recuperado de http://www.expansion.com/juridico/opinion/2016/05/24/5744979ee5fdeacd408b45e2.html. Último acceso 11 noviembre de 2016.

[228] Publicado en el DOCE el 4 de mayo de 2016.

actualizada que tenga en cuenta el impacto de las TIC. Todo ello ha inspirado la redacción del nuevo texto europeo[229]. Al mismo tiempo, se han venido tomando **decisiones de adecuación urgentes**, como el reciente "Escudo de Privacidad" o "Privacy Shield" entre la EU y EEUU, que se adoptó el 12 de julio de 2016, como mecanismo de conformidad en lo relativo a las transferencias transatlánticas de datos[230], y que reemplaza el acuerdo de "Puerto Seguro" que el TJUE invalidó en 2015[231]. Y que se puede considerar como una medida adicional para establecer un marco predecible para las transferencias de datos personales entre EE.UU. y la UE, que aporta seguridad jurídica y menores cargas administrativas (es decir, costes).

A la relevancia que estas medidas como el "Escudo de Privacidad", hay que tener en cuenta la herramienta jurídica elegida en esta ocasión para lograr la armonización que no consiguió la Directiva 95/46/CE; la aprobación de la nueva regulación vía reglamento debe desplazar las leyes nacionales de los Estados miembros, pero el enfoque del Consejo de la UE parece que apuesta más por suavizar dicho efecto, pues existo un margen de maniobra para los Estados miembros, frente a los otros textos de la Comisión y el Parlamento (Durán Cardo y García Morales, 2015).

Esta reforma iniciada en el año 2012 ha tenido un recorrido protagonizado por las **presiones de los lobbies de grandes empresas y gobiernos**, lo que da una idea de la trascendencia de la misma. La protección de datos, principalmente por su calidad de derecho instrumental, se ha convertido en pieza central para proteger a los ciudadanos en el entorno digital. Al ser este un espacio global, exige que la protección se dirija no solo a empresas europeas. Por ello, se han adaptado los criterios de aplicación territorial del Reglamento para que se extienda a responsables ubicados fuera de la Unión Europea en función de unos puntos de conexión y almacenamiento de datos más adaptados a este contexto digital.

Así pues, el RGPD trae de facto en cualquier caso un desplazamiento normativo de las legislaciones de cada Estado miembro, como LOPD en España (en vísperas de su modificación), en todo aquello que se oponga a la nueva regulación europea. En principio las legilaciones nacionales no son derogadas, sino que seguirán en vigor a partir del 25 de mayo de 2018, hasta que se alcance su completa derogación o alternativamente su modificación para adecuarla al RGPD[232], como es el caso de la LOPD. Con la aplicación

[229] RGPD. Recuperado de https://iapp.org/news/a/el-rgpd-el-nuevo-reglamento-europeo-sobre-la-proteccion-de-datos-personales-basado-en-el-principio-de-accountability/. Último acceso 2 enero 2017.

[230] Comisión Europea. La Comisión Europea pone en marcha el "Escudo de Privacidad" UE-EE.UU. Recuperado de http://europa.eu/rapid/press-release_IP-16-2461_es.htm. Último acceso 5 enero 2017.

[231] El Caso Schrems se inició en el año 2013 en Irlanda, donde Facebook tiene su filial europea, cuando el austríaco Maximilian Schrems interpuso una denuncia ante la autoridad del país de protección de datos a partir de las revelaciones de Edward Snowden relativas a las actividades de la NSA y el programa PRISM, alegando que sus datos personales como usuario de Facebook no estaban protegidos (una vez que eran enviados y guardados en los servidores fuera de la UE).

[232] Asunto sin lugar a dudas controvertido, pues el RGPD no puede derogar una ley, facultad que en principio corresponde a los parlamentos nacionales.

del RGPD van a aumentar los perjuicios que potencialmente puede llegar a sufrir una empresa, y que abordo más adelante.

La intención de los legisladores de la UE es armonizar las distintas normas nacionales de protección de datos a través de normas directamente vinculantes para todos los Estados miembros, algo razonable en la evolución hacia un mercado libre dentro de la UE, como acertadamente apuntan Ploem, Essink-Bot y Stronks (2013); este objetivo en su opinión está alineado con los deseos de facilitar la investigación a nivel europeo por la comunidad médica de investigadores, y citan como ejemplo la Infraestructura de Investigación Biobancaria e Biomolecular de la UE (BBMRI)[233], que representa uno de los proyectos europeos pioneros, diseñado para fomentar y dar apoyo a una infraestructura de investigación paneuropea; la predisposición hacia el desarrollo de biobancos en Europa es positiva en general, pero la gran mayoría de los biobancos son todavía desconocidos para la gran mayoría de ciudadanos. Por lo que se hace necesario que los biobancos participen más activamente en iniciativas de diálogo con la ciudadanía.

Como afirman Fears et al. (2014) se hace necesario en este momento establecer el **equilibrio entre el bien público derivado de la investigación en salud y la protección del individuo**, para que los pacientes y el ciudadanos en general puedan continuar beneficiándose de los avances científicos y aprovechando la experiencia adquirida en distintos centros europeos de excelencia para el procesamiento de datos; se hace necesario así diseñar un marco regulador razonable que sea suficientemente flexible cómo para hacer frente a los cambios futuros en la recopilación, el análisis, la ampliación y la transferencia de datos.

La mayor parte de nuestro conocimiento actual sobre enfermedades, así como los ensayos de diagnóstico y los fármacos disponibles, se han obtenido a través de la investigación sistemática de muestras biológicas humanas y datos médicos; como afirman Van Ommen et al. (2015) una de las claves de estas investigaciones es la posibilidad de obtener acceso estructurado a muestras y datos de pacientes donantes con controles de calidad, un acceso respetuoso con los principios éticos y con las normas de privacidad establecidas en los países participantes. El consorcio BBMRI-ERIC tiene como objetivo mejorar la accesibilidad y la interoperabilidad entre el mundo académico y el industrial para beneficio de la medicina

[233] BBMRI (Biobanking and Biomolecular Resources Research Infrastructure) constituye uno de los primeros proyectos de Infraestructuras de Investigación de la EU financiados por la Comisión Europea; la fase preparatoria terminó en enero de 2011. Durante los últimos 3 años BBMRI se ha convertido en un consorcio de 53 miembros con más de 280 organizaciones asociadas (en su mayoría biobancos) de más de 30 países, llegando a representar el mayor proyecto europeo de infraestructura de investigación. Durante la fase preparatoria se formuló el concepto de biobanco funcional pan-europeo y ha sido presentado a los Estados miembros de la UE y a los estados asociados para su aprobación y financiación. BBMRI formará una interfaz entre especímenes y datos (de pacientes y poblaciones europeas) y de investigación biológica y médica de alto nivel; esto sólo puede lograrse mediante una infraestructura de investigación distribuida con unidades operativas en todos los Estados miembros participantes. BBMRI se ejecutará bajo la entidad legal ERIC (European Research Infrastructure Consortium). BBMRI-ERIC prevé que la sede (coordinación central) esté situada en Graz, Austria, y será responsable de la coordinación de las actividades de los Nodos Nacionales establecidos en los países participantes. (https://www.structuralbiology.eu/resources/organisations/bbmri-biobanking-and-biomolecular-resources-research-infrastructure).

personalizada, la prevención de enfermedades para promover el desarrollo de nuevos diagnósticos, dispositivos y fármacos.

Sethi (2014) destaca el papel crucial que desempeña la farmacoepidemiología para la seguridad de los pacientes y por qué el acceso a los datos es clave para facilitar esta investigación; la farmacoepidemiología implica "el estudio del uso y los efectos de los fármacos y otros dispositivos médicos en gran número de personas" con el objetivo es examinar todos los efectos que se puedan detectar, ya sean beneficiosos o adversos, e incluye actividades diversas como el estudio de reacciones adversas a los fármacos. Por otro lado, el aumento del volumen de datos proporcionados por la secuenciación del ADN y otros métodos de alto rendimiento, como bien apuntan Galli et al (2015), también vendrán a proporcionar un desafío constante para la computación y recursos bioinformáticos.

Existe por lo tanto unos claros desafíos bajo la nueva legislación europea, como apunta Hatfield (2016) las empresas con sede en EE.UU. tendrán que adaptarse no sólo la estructura de sanciones que será más prohibitiva, sino que también se perderán muchas de las ventajas actuales, como ocurrió con el principio de "Puerto Seguro" o "*Safe Harbor*"[234] [235] al pasar a no ser reconocido como una protección legítima por la UE[236], lo que ha obligado a los recopiladores de datos a **cambiar sus políticas de transferencia de datos y de almacenamiento**, como ha sido el caso con el contenido de las políticas de datos de Facebook (Gómez Múñoz y Cañabate Pérez, 2016), por ejemplo; según cifras que proporciona el diario Financial Times unas 4.400 compañías[237] están adheridas a este acuerdo de "Puerto Seguro"; entre ellas se encuentran las grandes multinacionales tecnológicas como Google, Amazon, Twitter, Facebook, Apple, Microsoft...[238]. En los últimos años se han producido denuncias por parte de ciudadanos europeos debido a las injerencias crecientes por parte de las autoridades estadounidenses (incluida la NSA), lo cuál ha tenido impacto directo en las empresas estadounidenses que se enfrentan a la disyuntiva de cumplir con las exigencias de protección y privacidad impuestas por el régimen de la UE o bien atender las demandas de

[234] La Comisión Europea, a través de su Decisión de 26 de Julio de 2000, y de acuerdo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, se había pronunciado sobre la adecuación conferida por los principios de "Puerto Seguro" para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EE.UU. www.agpd.es. Último acceso 5 enero 2017.

[235] El principio "Puerto Seguro" tenía la intención de cerrar la brecha entre los dos regímenes (UE/EE.UU.) para permitir que las compañías no europeas, y estadounidenses en particular, alcanzaran un nivel de protección aceptable por la UE, que autorizaba a las compañías no europeas la transferencia de datos de carácter personal a un tercer país cuando garantizasen un nivel de protección adecuado y se respetase las disposiciones legales de los Estados miembros -aunque la en la práctica no se pudiese comprobar el nivel de protección-, pero con el nuevo Reglamento, esas compañías tendrán que mantener el cumplimiento con dos protocolos separados.

[236] El 6 de octubre de 2015 el Tribunal de Justicia de la UE dió un paso más para proteger la privacidad de los usuarios y consumidores europeos con la anulación del conocido "Puerto Seguro"; el acuerdo de "Puerto Seguro" (por el cual las compañías podían transferir datos de sus usuarios europeos a EE.UU. para tratarlos o almacenarlos), ha sido invalidado, por lo que los tribunales de cada Estado miembro tienen vía libre ahora para declarar, si este tratamiento de los datos personales de sus ciudadanos es o no legal; la referida sentencia afirma que: "…la existencia de una Decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y de la Directiva."

[237] Data Protection: No Safe Harbour. Recuperado de https://www.ft.com/content/f2ecc7ca-6e65-11e5-aca9-d87542bf8673. Último acceso 2 diciembre 2016.

[238] La lista de las empresas adheridas se puede consultar en este enlace: https://safeharbor.export.gov/list.aspx. Último acceso 3 diciembre de 2016.

diversos organismos gubernamentales estadounidenses de entrega de información; el nuevo acuerdo "Escudo de Privacidad" o "Privacy Shield" conlleva que las empresas norteamericanas que almacenan datos de ciudadanos europeos, están **obligadas a certificar cada año** que son respetuosos con el acuerdo, resuelven las quejas que se le formulen, y cooperan en el cumplimiento con las autoridades europeas de protección de datos. El "Escudo de Privacidad" debe solventar las deficiencias que acabaron con el "Puerto Seguro", y **permitir el flujo seguro de datos personales** entre la UE y EE.UU. (Weiss y Archick, 2016).

Weiss y Archick (2016) abordan las medidas de reforma de la protección de datos de la UE, cuya nueva reglamentación actualiza la Directiva de 1995, y destacan que cubrirá la mayor parte del procesamiento de datos personales tanto en el sector público como en el privado; este Reglamento, que será directamente aplicable en todos los Estados miembros de la UE (frente a las actuales normas armonizadas), constituye un conjunto único de normas iguales para todos los Estados miembros de la UE. Por lo tanto el nuevo RGPD persigue proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su **derecho a la protección de los datos personales tanto si son procesados por entidades privadas como por administraciones públicas, algo muy novedoso de esta nueva regulación**, Además, no sólo se reconocen los clásicos derechos de acceso, rectificación, cancelación y oposición, sino que también se aborda la regulación de dos nuevos derechos, por un lado el llamado derecho al olvido (entendido como efectivo derecho de supresión), y la portabilidad de los datos[239]. También se profundiza, con mayor detalle, en las garantías para los interesados, especificaciones y excepciones del deber de información, los deberes de transparencia o la limitación del tratamiento de datos personales con fines de archivo en interés público, de investigación científica e histórica, bien con fines estadísticos.

Conviene destacar otra novedad práctica relevante, la aplicación del RGPD al procesamiento de datos de europeos por entidades establecidas en Europa, y también por las **empresas ubicadas fuera de la UE que operen dentro del territorio de la UE** y cuya actividad suponga el tratamiento de datos personales, a pesar de que puedan no tener presencia física en el ámbito geográfico de la propia UE; además, hay que añadir la obligación que se impone sobre empresas y administraciones públicas para nombrar, en ciertas circunstancias, a un "data protection officer" (DPO) o delegado de protección de datos, que garantice el cumplimiento del Reglamento. Hay que destacar el papel del DPO, independiente del Responsable de Seguridad, y con exclusividad en sus funciones; es necesario que el DPO sea elegid de acuerdo tanto a sus cualidades profesionales como a sus conocimientos normativos y prácticos especializados que deben estar debidamente acreditados. Por último, hay que mencionar los **importes del nuevo régimen sancionador (artículo 83 del RGPD), que ascienden considerablemente para llegar a €20.000.000 o el 4% del total**

[239] Hoy entra en vigor el reglamento de protección de datos en toda Europa. Recuperado de http://www.expansion.com/juridico/opinion/2016/05/24/5744979ee5fdeacd408b45e2.html. Último acceso 11 noviembre de 2016.

anual global del volumen de negocio en el último ejercicio financiero (infracciones graves), o para infracciones leves €10.000.000 o el 2% de la facturación anual global.

Auffray et al. (2016) denuncian, por otro lado, la ausencia aún en la UE de una armonización en el formato de los datos, en su procesamiento, análisis y transferencia, lo que conlleva incompatibilidades y pérdida de oportunidades. Los marcos legales referidos a la cesión de los datos están evolucionando; personal sanitario, investigadores y ciudadanos requieren de mejores métodos, herramientas y formación para generar, analizar, y solicitar datos de forma efectiva; abordar estas barreras contribuirá a crear un mercado europeo único en salud, que mejore la salud y la atención sanitaria de los europeos. Sin embargo, Currie y Seddon (2014) advierten que un mismo enfoque en materia de salud y TIC no resulta aconsejable para los Estados miembros de la UE debido a que los responsables de formulación de políticas a nivel nacional tienen que desarrollar una hoja de ruta de *eHealth* que refleje las condiciones nacionales, regionales y locales, que van más allá de los imperativos técnicos.

La aplicación del Reglamento 2016/679 de protección de datos[240] en 2018 tendrá efectos serios sobre las empresas, que pueden abarcar desde el daño reputacional a un elevado coste económico (sanción administrativa); dichas empresas serán sancionadas si ante una brecha de seguridad no informaran (en un plazo máximo de 72 horas) a los interesados o a la autoridad competente. Se impone por lo tanto la necesidad imperiosa de adaptarse a la nueva regulación antes del 25 de mayo de 2018.

Al mismo el RGPD viene acompañado otras transformaciones como la Directiva 2016/1148 del Parlamento y del Consejo Europeo, aprobada el 6 de julio de 2016, ya conocida como NIS[241] Europea, que tiene como fin garantizar un nivel elevado y común de seguridad de las redes y sistemas en la UE (**ciberseguridad**), al margen de lo que cada Estado miembro determine de forma específica como medidas adecuadas.

Son variadas las novedades más destacadas que acompañan al RGPD que se aplicará de forma directa a nivel paneuropeo (UE), que es por lo tanto transfronterizo. En empresas de más de 250 trabajadores se exige un "*Data Protection Officer",* que debe poseer una formación adecuada con conocimientos de Derecho y de Protección de Datos. Formará parte de la empresa pero puede ser colaborador externo. Sus funciones principales serán, a saber: (1) revisar una serie de actuaciones internas (2) informar y asesorar a los empleados de las organizaciones, que lleven a cabo tratamiento de datos, sobre las obligaciones que establece la normativa vigente (3) monitorizar los procedimientos establecidos en cada organización,

[240] AEPD. El Reglamento de Protección de Datos. Recuperado de https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php. Último acceso 15 enero 2017.

[241] Acrónimo del inglés *"network and information security"*

certificando que se adaptan a la normativa vigente sobre protección de datos (4) cooperar con las autoridades nacionales de protección de datos.

Los menores de entre 13 y 16 años (según lo que cada país determine como edad mínima) precisarán del permiso de los padres para abrir cuentas en redes sociales (como Facebook, Instagram o Snapchat etcétera), y las organizaciones deberán contar con la autorización de los padres o tutores, para poder hacer un tratamiento de datos personales de un menor, a la vez que el responsable de tratamiento se debe asegurar de que así ocurra.

En cuanto a derechos fundamentales se incorpora el derecho al olvido, cualquier persona tendrá derecho a que su información sea eliminada de los proveedores de servicios de internet cuando lo solicite (siempre y cuando no existan razones legítimas para retenerlos), y se consolidan en todo caso los derechos ARCO (acceso, rectificación, cancelación y oposición). Aunque para Mañas, Caro y Gayo (2016) el RGPD acaba con dichos derechos ARCO al introducir ahora los derechos de transparencia (artículo 12), información (artículo 13 y 14), acceso (artículo 15), rectificación (artículo 16), supresión o derecho al olvido (artículo 17), limitación del tratamiento (artículo 18), portabilidad de datos (artículo 20) y oposición (artículo 21).

Se crea una nueva categoría de datos especialmente protegidos como los referidos a la orientación sexual, los **datos genéticos, los biométricos,** o las creencias filosóficas. Y desaparece la necesidad de notificar los ficheros ante las distintas agencias nacionales de protección de datos, a la vez que se refuerza la necesidad de un consentimiento claro y afirmativo sobre el tratamiento de los datos personales, ya no es suficiente que se haga por defecto (casillas marcadas, silencio, inacción, etcétera). Por otro lado, los términos y condiciones tendrán que ser redactados en un lenguaje sencillo, y el responsable del tratamiento debe poder demostrar que se ha obtenido dicho consentimiento. Se impone la ventanilla única; las empresas sólo precisarán ponerse en contacto con **un único supervisor en Europa** (con el consiguiente ahorro de costes).

El RGPD impone el concepto de *"Privacy by Design"* o "Privacidad desde el Diseño" como hilo conductor, un consentimiento vertebrado, informado, es decir, que el titular de los datos entienda de verdad las consecuencias de su consentimiento; el RGPD trae consigo la aplicación simultánea de distintos principios que, aplicados en el ámbito de las "apps" (o aplicaciones), vienen a explicar la denominada atomización y vertebración del consentimiento; se trata de las nuevas solicitudes de permisos o "**mini consentimientos**" (si se me permite la expresión) para ejecutar acciones específicas[242]. Estos principios

[242] El consentimiento pasa a prestarse en pequeñas dosis (vértebras), que engarzan entre sí, para que de esta manera se pueda prestar el consentimiento para fines específicos.

generales son la privacidad por defecto (el sistema debe funcionar de la forma más respetuosa para la privacidad del usuario, hasta el momento en que éste autorice otra cosa de forma activa), privacidad integrada en el diseño (es decir, en vez de ser aplicarse a posteriori, por defecto la privacidad debe quedar integrada en el sistema) minimización de datos (reduciendo al mínimo necesario los datos a tratar, el ámbito del tratamiento, el tiempo de custodia y el acceso de terceros -artículos 5 y 25 del RGPD-), transparencia (que la política de protección de la privacidad -de cualquier empresa, servicio, o sistema- sea pública y pueda verificarse por los propios usuarios y el resto de agentes interesados), y empoderamiento del usuario (es decir que el individuo tenga el control último, incluidos los tratamientos de terceros)[243].

Se trata por lo tanto del **fin del consentimiento tácito** al tratamiento de datos, y esto es una novedad trascendente del RGPD; queda prohibido apreciar que se ha otorgado el consentimiento (en determinados casos) aún cuando el titular no se oponga expresamente al tratamiento, y con ello se acabó también cesiones de datos a terceras empresas (ligadas o no) al servicio que origina el consentimiento. De acuerdo con el RGPD cualquier tratamiento requiere como soporte un consentimiento expreso, a la vez que el responsable del tratamiento debe poder acreditar ese consentimiento (Mañas, Caro y Gayo, 2016). Según la AEPD además los responsables de datos tendrán que "regularizar" aquellos consentimientos tácitos recabados hasta ahora, aunque no se ha definido todavía cómo se hará. En todo caso, y volviendo al planteamiento -si cabe más filosófico, y no por ello menos pragmático- de Han (2015) y su sociedad de la transparencia, nos encontramos aquí con la paradoja de la transparencia; la simplificación de la información que se ofrece a quién debe prestar un consentimiento informado, siempre y cuando la información sea leída (aunque la meta última sea que el usuario comprenda las implicaciones de dicho consentimiento).

El artículo 25.2 del RGPD impone 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. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad."* Se hace por lo tanto necesario la colaboración de los responsables de los distintos departamentos de la empresa, para analizar los flujos de datos y su adecuación al control por parte del usuario.

Apartir de 2018 así pues se abre un nuevo escenario, cuando finalice esta etapa de transición hacia un más complejo y nuevo marco normativo de la privacidad en Europa, que traerá cambios para los ciudadanos y desde luego para el tejido empresarial; en el futuro será preciso extremar la ponderación de las circunstancias que concurran en cada supuesto concreto para decidir sobre la legitimidad del tratamiento de

[243] García Herrero, J. (22 enero 2017). Jorge García (blog). Recuperado de http://jorgegarciaherrero.com. Último acceso 31 enero 2017.

datos, pero parece razonable concluir que se producirá una convergencia de las políticas de protección de datos en la UE; la nueva regulación debería eliminar las divergencias y costes asociados para las empresas. Uno de los grandes proyectos de la UE en materia sanitaria es la accesibilidad global de los datos a través de la HCE[244]; el nuevo RGPD[245] incluye novedades como el endurecimiento del régimen sancionador, a la vez que se pretende impulsar la economía digital y la Innovación. Se propone por primera vez en casi 20 años reforzar la actual normativa, lo que va a representar el paso de una regulación vía directiva a una regulación vía reglamento (directamente aplicable en los Estados miembros). Pero no son pocas las barreras a las que se enfrenta esta reforma, incluidas las diferencias culturales entre Estados miembros, factor importante a la hora de desarrollar un marco jurídico armonizado.

[244] Iniciada en 2012 cuando la Comisión Europea propuso la reforma para armonizar la forma en se recogen los datos, su acceso y uso, en el marco de la economía digtial.

[245] El 12 de marzo de 2014 el Parlamento Europeo dio luz verde al proyecto de Reglamento Europeo de Protección de Datos, cuyo texto final fue publicado en el Diario Oficial de la Unión Europea el 4 de mayo de 2016.

Capítulo 5. Conclusiones, Limitaciones y Futuro.

5.1. Conclusiones.

5.1.1. Protección uniforme como garantía para la investigación internacional.

Esta investigación ha analizado las principales características del actual sistema de protección de datos aplicable al área de *eHealth* en la UE y las diferencias que existen entre éste y otros sistemas no comunitarios, especialmente América Latina. En este sentido, esta investigación destaca los principales elementos que han conducido a la armonización en Europa y que han determinado la configuración de este derecho en otras jurisdicciones. Como señala Hoofnagle (2016) las transposición de la Directiva de 1995 ha invitado a ciertas desviaciones respecto a lo que es una norma uniforme, pero **el RGPD se cree va a tener un efecto unficador (acompañada de enormes reducciones de costes).**

La primera conclusión que se desprende de esta investigación es que la verdadera integración en la política de protección de datos en la UE debería llegar a partir de 2018 con la aplicación de la nueva regulación; lo que nos demuestra el hecho que hasta ahora cada Estado Miembro ha desarrollado la Directiva de 1995 de forma similar pero no idéntica, y sólo a partir de entonces podremos ir analizando cómo se extiende la política unificada de la UE. **La armonización integral** en la UE no será fácil a pesar del RGPD pero debe traer claridad y consistencia: las mismas normas serán de aplicación directa a todas las compañías que quieran operar en la UE, independientemente de dónde se encuentren; los ciudadanos podrán tener mayor confianza[246] en el tratamiento de sus datos personales y para esta protección confían en las instituciones europeas más que en las nacionales. Así, la protección uniforme en el espacio europeo servirá de garantía de la libertad para el ciudadano en Europa, frente a países como EE.UU. donde la libertad del individuo parece quedar supeditada a intereses mercantilistas o de agencias del gobierno. La UE se ha posicionado a favor del avance tecnológico y del recorte de costes, ventajas que ofrece la armonización. En este sentido, Rothstein (2015) defiende la armonización de las leyes de privacidad para hacer posible además la investigación internacional con datos de salud, y más concretamente con biobancos.

5.1.2. La armonización internacional, una tendencia liderada por los europeos.

En el entorno actual del Big Data el objetivo principal de esta investigación consistía en constatar una tendencia liderada por los propios ciudadanos hacia la homogeneización en Europa de los parámetros a

[246] Con este fin se creó el *Online Privacy Alliance (*www.privacyalliance.org) por empresas y asociaciones como un grupo para la autoregulación en materia de privacidad, para crear un ambiente que genere confianza y promueva la protección de la privacidad de los clientes, específicamente en el marco del comercio electrónico. Está integrado por empresas como Nestlé, Microsoft,, eBay Inc., Dell, Boeing, AT&T, Apple Computer, AWS Convergence Technologies Inc., EDS, PricewaterhouseCoopers, Time Warner Inc., Verizon Communications, The Walt Disney Company, etcétera.

los que se debe adecuar la salud digital en relación con la protección de datos. La Directiva de 1995 consagraba dos de los principios más antigüos y relevantes del proceso de integración europea; por un lado la protección de los derechos y las libertades fundamentales del individuo y, por otro, la **consolidación de un mercado interior, que incluye la libre circulación de datos personales.** Los rápidos cambios tecnológicos y la globalización han cambiado radicalmente nuestro entorno, sin embargo, más de 20 años más tarde, este doble objetivo sigue estando en vigor y los principios reconocidos en aquella Directiva siguen siendo tan válidos y sólidos. Un armonización de la normas de privacidad además tendrá beneficios para la investigación transfronteriza con biobancos (Rothstein y Knoppers, 2016; Rothstein, Knoppers y Harrell 2016).

Ejemplos de armonización internacional liderada por Europa y la UE hay varios en esta investigación; al establecer unas medidas o controles de seguridad en la nube pública, baste mencionar la norma ISO 27018, basada principalmente en regulaciones y leyes emitidas por la UE. Como se ha verificado, anteriormente los proveedores de la nube pública, por ejemplo, sólo podían certificarse, en cuanto a seguridad, a través de las normas ISO 27001, pero esta norma llega más lejos y debe valorarse justamente no sólo un estándar internacional, sino un código de buenas prácticas, con aplicación directa en el tratamiento de los datos y el área *eHealth*.

5.1.3. Lo que ocurre en Europa no permanece en Europa.

Otra conclusión que podemos confirmar es que **lo que ocurre en Europa no permanece en Europa**, en mayor o menor grado, tal y cómo se deriva de los datos recogidos en esta investigación; baste aquí citar como ejemplo las investigaciones de Greenleaf (2012, 2014, 2016) relativas a la influencia del Convenio 108 del Consejo de Europa. Tanto la privacidad como la protección de datos y la salud se han analizado en esta investigación desde distintos puntos de vista. A la vista del "tsunami" de Big Data de salud que se avecina y los crecientes nuevos modelos de negocio, parece que la tendencia pasa por otorgar, si cabe, un mayor control a las personas sobre sus datos, en línea con la regulación europea. El primer paso para ayudar a los individuos a poder ejercitar un mayor control sobre sus datos es su derecho a acceder a todos los datos que cualquier organización posea sobre ellos.

Por otro lado, las iniciativas basadas en poner el nuevo foco de atención sobre el uso de los datos (y no tanto sobre la recogida de los mismos) otorgan mayores responsabilidades a las empresas. Por ello algún autor, crítico con el modelo europeo, ya ha propuesto nuevo modelo de negocio basado en el empoderamiento del individuo, como agente económico que gestiona su propia información, para sus

propios fines, y comparte una parte de esa información con las empresas para comunicar qué quieren, cómo y cuándo, para obtener beneficios conjuntos (Rubinstein, 2013).

Para Castells (2014) estamos viviendo un fenómeno histórico trascendente, que consiste en la **"construcción de una red global de comunicaciones basada en Internet",** aunque no estoy de acuerdo en que esta tecnología encarne la cultura de la libertad en la que se originó como afirma Castells; realmente creo que en muchos aspectos, nuestros datos personales, que ya no sólo figuran en papel, se encuentran cada día en un mayor número de formatos y archivos, almacenados en no sabemos qué lugar, y accesibles por no sabemos qué organizaciones, aseguradoras, gobiernos, empleadores, etcétera. Por ello se hace necesaria una regulación armonizada, que imponga límites y barreras al acceso y uso de los datos personales más allá de las fronteras del país en donde vivimos.

En relación al modelo europeo de normalización, el mismo ETSI, se estableció originalmente para desarrollar estándares europeos, pero como afirman Van de Kaa y Greeven (2016) su trabajo e influencia cada día va más allá y se está dirigiendo hacia el desarrollo de otro tipo de normas, incluyendo normas internacionales, y tanto empresas como universidades e institutos de investigación, de un amplio espectro de países fuera de Europa, se han incorporado al mismo.

Young (2015) destaca el impacto en distintos sectores del sistema regulatorio de la UE fuera del territorio comunitario, lo que define a la UE como un **agente global**, pues entiende que la regulación de la UE afecta a la forma en que se desarrollan las empresas y los consumidores, y al ámbito de protección en distintas partes del mundo más allá de sus fronteras. Para Young existe un consenso amplio sobre el enorme poder regulatorio que encarna la UE (Lavenex, 2014; Scott, 2014; Vogel, 2012; Drezner, 2007; Sapir, 2007). Bradford (2012) llega a afirmar que **la UE es el regulador predominante del comercio mundial**, algo que también defienden Jacoby y Meunier, 2010; Posner, 2009. En todo caso, la influencia regulatoria de las políticas de la UE ha despertado gran interés y ha sido ampliamente analizada[247].

Se trata de una forma de globalización legal, donde una jurisdicción (entendido como país o conjunto de Estados) induce a otros países a adoptar mecanismos legales similares sin coerción; es lo que Birnhack (2008) define como un **mecanismo no coercitivo de globalización jurídica suave**, que ejemplifica con la Directiva de la UE sobre protección de datos personales y su mecanismo para la exportación de dichos datos. Se refiere al artículo 25 que regula la transferencia de datos a un tercer país sólo si dicho país garantiza un nivel adecuado de protección de datos. Esta norma, que he abordado anteriormente, conlleva que aquellos países que pretendan intervenir en transacciones de datos con Estados

[247] también por la prensa internacional, como hacen Lipton y Hakim (2013) en el NY Times, y Mitchener (2002) en el Wall Street Journal.

miembros de la UE deben estar reconocidos como garantes de un nivel adecuado de protección. Coincido con Birnhack en que la Directiva ha tenido un impacto global mucho mayor de lo que se ha reconocido y que hoy se erige como el **principal motor de un régimen mundial emergente de protección de datos.** Así, podemos afirmar que la UE desempeña un papel de liderazgo en el proceso de concentración en materia de protección de datos, dentro del movimiento actual de creciente globalización.

La propia Comisión Europea (2007) en su documento de trabajo "*The external dimension of the Single Market review'*, habla de ampliar el espacio regulador del mercado único, mediante la **proyección de las normas y los valores comunitarios en el exterior**, permitiendo que las regulaciones europeas se beneficien de las mejores prácticas que existan por todo el mundo, para hacer de las normas europeas una referencia para los estándares internacionales. Ya entonces la Comisión quería reforzar la idea de la UE como un legislador a nivel global. Es decir, la Comisión no se conforma con marcar las pautas para el respeto a los valores y normativas europeos, sino que aboga claramente por extender su visión y sus principios a nivel global.

Por lo tanto, puedo concluir que no cabe duda de que las normativas de la UE tienen efectos más allá de las fronteras del mercado único, influyendo notablemente en América Latina (Delgado 2014; Greenleaf, 2014; Schwatrz, 2013; Arellano Teledo, 2012), a la vez que el modelo europeo se erige como **un modelo con influencia transfronteriza más allá de la UE** pudiendo considerarse un modelo líder a nivel global (Craig y Ludloff, 2011; Greenleaf, 2012).

5.1.4. Oportunidad para nuevos modelos de negocio.

Así los códigos de conducta (Dean, Payne y Landry, 2016) a los que las empresas se adhieran serán relevantes, para cumplir con la normativa en vigor, pero las propuestas de los nuevos modelos de negocio pueden aportar soluciones innovadoras. Teniendo en cuenta que las mayores organizaciones de Big Data a nivel mundial no provienen de la UE parece razonable que la reforma legal vaya acompañada de un estímulo para el desarrollo de nuevos modelos de negocio que protejan al consumidor y que permitan a las empresas (que cada día recogen más y más datos) **beneficiarse lícitamente del uso de los datos** para ofrecer nuevos servicios. Así, el acuerdo "Escudo de Privacidad" permitirá a las empresas estadounidenses disponer de un marco predecible almacenar datos de ciudadanos europeos, a la vez que para estos representa mayor transparencia en relación con las transferencias de datos personales. Se trata de un nuevo marco legal para la cesión de datos con importantes consecuencias comerciales.

En consecuencia, como defiende Rothstein (2015) respecto a la investigación internacional con datos de salud, existen razones de peso para que las grandes compañías de tecnología de información estadounidenses (por ejemplo) resuelvan el problema de la transferencia de datos y se adhieran al acuerdo de "Escudo de Seguridad"[248], antes de que su posición competitiva se vea socavada. Y es que precisamente el cumplimiento de las obligaciones en materia de protección de datos de carácter personal puede convertirse en una **ventaja competitiva, como la citada ISO 27008, pues permite conocer si el proveedor de servicios ha tomado medidas de protección de datos personales** (auditables y verificables por terceros). En este sentido, ante la próxima aplicación del RGPD, los códigos de conducta sectoriales se van a transformar en una herramienta muy útil y necesaria, en el contexto de la mayor protección y seguridad jurídica de los particulares que se avecina.

Se constatan oportunidades de mejora en lo relativo a convergencia, pero también en materia de competitividad de los modelos de negocio basados en *eHealth*; constatación de que los riesgos de explotación (posibles demandas de los usuarios) se pueden reducir drásticamente, así como los costes económicos de explotación de los nuevos modelos de negocio de eSalud (sanciones impuestas como consecuencia de la vulneración efectiva del derecho a la protección de datos); la reputación de los nuevos modelos de negocio (redes sociales más seguras para los usuarios) y su credibilidad están vinculadas a las garantías y controles que puedan ofrecer; los nuevos modelos de negocio para ser sostenibles deberán aplicar un modelo de calidad de datos[249]. La UE puede establecer de forma efectiva un marco estándar para una gama más segura de productos de consumo en todo el mundo (Terstegge, 2017).

Hablaba Han (2013) de la ideología del conocimiento que se sustenta en la explotación de la transparencia, del acopio de información y datos de todo tipo que fluyen por las redes y sistemas de la información. Pero Vásquez Rocca (2015), que comparte un planteamiento similar, se aparta de su visión precisamente en este aspecto, pues considera que en el fondo la tecnología nunca ha sido tan opaca (en su opinión, deliberadamente) como es el caso hoy en día, haciendo referencia a los fabricantes de móviles, ordenadores, tablets, etcétera, que nos presentan productos digitales aparentemente atractivos y bien diseñados, pero herméticos, sin poder siquiera acceder físicamente a su interior[250], el lenguaje del software es complejo, la escritura de programación está encriptada, el lenguaje cifrado, los circuitos de software resultan inaccesibles, etcétera, lo que convierte en opacas e inaccesibles a estas herramientas. Para acabar con la opacidad, también, en materia de protección de datos, conviene que los nuevos modelos de negocio se

[248] La Comisión Europea presentó el primer borrador el 29 de febrero de 2016 y, el Parlamento Europeo adoptó la resolución de aprobación el 26 de mayo del mismo año. El 8 de julio los representantes de los Estados miembros aprobaron la versión final del *"EU-US Privacy Shield"*. El plazo para que las empresas y entidades de los EE.UU. presenten sus auto certificaciones ante el Departamento de Comercio de EE.UU. se abrió el 1 de agosto de 2016.

[249] De acuerdo con el artículo cuarto de la LOPD que regula la calidad de los datos y establece los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales.

[250] Vásquez Rocca recoge que los últimos modelos de Mac y los iPhone no tienen tornillos, y por lo tanto no pueden abrirse a no ser que se acuda a sus tiendas y técnicos oficiales.

sometan códigos de conducta, códigos tipo, o normas internas al margen de los que estipule la legislación en cada jurisdicción donde operen.

5.1.5. Derecho internacional consuetudinario.

La vigilancia masiva y el acceso a datos e información de particulares, y la creciente regulación a nivel global de la privacidad y la protección de datos personal, nos llevan a concluir que se está consolidando un concepto, universalmente reconocido, relativo a la protección de datos, una especie de **derecho internacional consuetudinario** (Zalnieriute, 2015), que desde luego no podemos concluir pueda ser ejercitado como derecho en la mayoría de jurisdicciones todavía, aunque ya se comienza a hablar de una ley internacional que proteja la privacidad.

Por otro lado, se encuentran normalmente tipificados en la propia LOPD (o en su Reglamento de desarrollo), los delitos en materia de tratamiento indebido de datos personales; algo que cómo bien señalan García y de los Ángeles debe por sí mismo representar un incentivo para el cumplimiento de las normas (a la vez que requiere se comiencen a aplicar las multas y las tipificaciones de delitos para que la normativa se cumpla, y evitar que se vulnere deliberadamente). En este sentido no puedo estar más de acuerdo en la necesidad de la aplicación de la capacidad sancionadora de los organismos reguladores, pues en última instancia este es un derecho de corta existencia todavía que requiere una mayor, si cabe, actividad fiscalizadora para la lograr la normalización de la cultura de la protección de datos (Mañas, 2009) que en gran medida lleva implícita la **homogeneización de la protección de datos**.

5.1.6. Ventajas del modelo de la UE versus el modelo de los EE.UU.

En este contexto se puede afirmar, como destaca Schwartz (2013), que la UE se enfrenta inexorablemente al modelo norteamericano (y sus grandes multinacionales de minería de datos) con políticas menos restrictivas, sino que además el nuevo Reglamento parece que irá más allá del actual status quo en materia de privacidad entre la UE y EE.UU., aumentando el distanciamiento; la UE se ha caracterizado por su escepticismo sobre el nivel de protección que las leyes norteamericanas otorgan, y terceros países a la vez parecen haber seguido el estilo de la UE referido al modelo de las llamadas leyes de protección de datos. El nuevo Reglamento parece que altera el cierto equilibrio existente, centraliza el poder en la Comisión Europea y amenaza las políticas de armonización existentes.

La protección de datos personales no se trata exclusivamente de una materia de derechos fundamentales. Para América Latina y muchos otros países por todo el mundo se trata de todo un dilema

importante, como apuntaba Gregorio (2004), Europa *versus* EE.UU.; se trata de las **implicaciones comerciales que seguir o no el modelo europeo (UE)** de protección de datos. Los tribunales están delimitando el funcionamiento de las grandes empresas que operan en Internet y facilitan el acceso libre a la información. **Quedar fuera del área de transmisión segura de datos (según criterios comunitarios), incluyendo el comercio electrónico, puede tener serias consecuencias para las organizaciones** que no se acomoden específicamente a la normativa de la UE en este materia (como ha demostrado el caso Schrems[251]), o a la normativa europea en su sentido más amplio; en esta precisa dirección actuó Rusia, que el 17 de noviembre de 2016 bloqueó la red social LinkedIn (propiedad de Microsoft), por violar las leyes rusas de acuerdo con el órgano de control de medios ruso, Rodkomnadsor[252]. Es la primera gran red social que se ha bloqueado en el estado ruso y sienta un precedente importante de cara a otras grandes compañías que operan en Internet en Europa. Se acusa a LinkedIn de almacenaje ilegal de datos de usuarios en servidores ubicados en el extranjero. De acuerdo con la actual legislación de la Federación Rusa, cualquier información relativa a ciudadanos rusos debe almacenarse en servidores locales por razón de seguridad, especialmente después del escándalo de la NSA (Gallagher y Greenwald 2014; Greenwald 2013).

En tiempos del Big Data y de la sociedad del conocimiento, la protección de los derechos de los usuarios (elemento básico de un código de buen gobierno) debería ser el activo principal de cualquier empresa (especialmente en el ámbito *eHealth*), no sólo para evitar los riesgos aquí analizados, sino para que se puedan tomar decisiones más inteligentes y estratégicas, que generen nuevas oportunidades a la hora de atraer nuevos usuarios y desarrollar con éxito los nuevos modelos de negocio. Igualmente, para terceros países, ser reconocido por la UE como país con un nivel de protección adecuado es un requisito que **facilita la transferencia internacional de datos**, y que en consecuencia ofrece mayores garantías para la protección de los derechos de las personas que genera ventajas competitivas, contribuyendo a consolidar o desarrollar nuevos negocios (Angarita, 2010).

Como afirma Angarita (2010) hay algunos muchos países como Colombia, que a pesar de sus reformas, aún no ha sido justamente considerado por la Comisión Europea como un Estado que garantiza un nivel adecuado de protección, pues entre otras razones la ley colombiana permite el flujo internacional de los datos sin garantías ni control en beneficio de los propios interesados (siendo la circulación internacional de datos un tema trascendental a la hora de mantener la calidad de protección de los datos personales de los ciudadanos); sin embargo, frente a la polaridad entre EE.UU. y la UE, Gregorio (2004) cree que **el enfoque**

[251] Que puso en evidencia la ausencia de reglas en EE.UU. que limitaran las posibles injerencias en los derechos fundamentales de las ciudadanos cuyos datos se transfirieran desde la UE y la falta de una protección jurídica eficaz contra intrusiones de terceros, al no disponer los ciudadanos de vías legales en ese país que les permitan acceder a los datos de su titularidad, para eventualmente lograr su rectificación o supresión (Gómez-Múñoz y Cañabate Pérez, 2016).

[252] Rusia bloqueó hoy la red profesional LinkedIn de Microsoft. Recuperado de http://www.elmundo.es/tecnologia/2016/11/17/582d7f44468aeb163d8b4585.html. Último acceso 8 diciembre 2016.

que mejor se ajusta (en materia de protección de datos) a la realidad de la región lationamericana, es la norma europea.

Habrá que atender a lo que ocurra en los próximos años, una vez que se aplique de forma efectiva el nuevo RGPD, para verificar cuál será la tendencia de terceros países. De momento, a través de organizaciones internacionales como ISO **se está produciendo alineamiento o suave armonización de las normas internacionales con el ordenamiento de la UE.** Serán las propias empresas y organismos (públicos y privados) los que, mediante un procedimiento de certificación específica de aplicación efectiva en su organización, conduzcan, o no, a una armonización *de facto* con los estándares de la UE**.**

5.1.7. Mayor protagonismo del individuo.

Es el individuo quién está en el centro de la protección de datos sensibles y debe ejercitar sus derechos si cree que están siendo vulnerados, aunque como sostiene De Marcos (2012) no tiene que ser un obstáculo para el desarrollo de la ciencia para su propio beneficio; por esta razón, el conocimiento sobre los parámetros de la protección de datos en el ámbito de la salud digital resulta fundamental entre el cuerpo de médicos, ingenieros, profesionales sanitarios y demás agentes implicados, en relación con los objetivos secundarios de la investigación.

Los consumidores y usuarios determinan cuáles son los límites que quieren poner a su privacidad; en última instancia, todo queda a expensas de las denuncias que los propios particulares puedan interponer en defensa de sus derechos e intereses (Pérez, 2015; Delgado, 2016), frente al **"gran hermano digital que monitoriza nuestros datos de salud"** (Kress, Monguet, Navarro y Moreno Reyes, 2015), lo que bien se podría identificar con la obra ***"Data and Goliath: the hidden battles to collect your data and control your world"*** (Schneider, 2015), o la lucha titánica de David (el individuo) con el Big Data. En este sentido el nuevo RGPD no sólo es un hito en la armonización paneuropea (a escala de la UE) de las leyes nacionales en este materia, sino que otorga mayor protección y seguridad jurídica a los particulares en defensa de sus derechos.

Redefinición de la relación profesional sanitario-paciente, en la uso y acceso a la información. Todo ello viene confirmado por el creciente grado de acceso a Internet como fuente de información sobre salud[253]. Si hay algo que no se puede parar es el fenómeno de las redes sociales, no sólo como herramienta de comunicación global, sino como instrumento de comunicación bidirecional en el ámbito de la salud. La

[253] Como recogido los datos de la encuesta de la Comisión Europea "Flash Eurobarometer 404" (2014).

creación de esta redes digitales y su desarrollo marcarán importantes transformaciones en este siglo, mayores seguramente que la Revolución Industrial de finales del siglo XIX. No hay duda que las redes sociales en Internet cambiarán (ya están cambiando) las acciones de gobiernos y empresas, puesto que incorporan un nuevo concepto: la democratización de la información; este término es revelador de los cambios que veremos en el futuro, ya que no serán los profesionales, ni las leyes sólo quiénes ejerzan su influencia, sino también y muy especialmente los ciudadanos. Este movimiento debe ser entendido como una forma de movilización, que surge de manera altruista y espontánea, al contrario de las acciones procedentes de los gobiernos o del sistema sanitario público. El futuro de la medicina parece quedar en nuestras manos, en nuestros dispositivos móviles, en nuestras aplicaciones de salud en general. Aquí debemos incluir ámbitos como el deporte, la alimentación, consumo, educación, etcétera; a pesar de los beneficios derivados de **la democratización de la medicina** (a través de la tecnología), habrá sectores del *"medical establishment"* que se resistan a los cambios, a la vez que la medicina a distancia abre importantes cuestiones relativas a las privacidad (Topol, 2015). Todo ello porque existe un enorme número de fuentes, recursos y herramientas digitales que podemos consultar libremente; se trata de un **acceso libre a la información**. Aquí está la clave la evolución en materia de salud; la democratización de la información antes reservada a médicos y profesionales sanitarios. Aunque para algunos investigadores, la tecnología tiene limitaciones sistémicas que influyen el potencial democratizador de los todos los medios (Papacharissi, 2010).

Bollier y Firestone (2010) abordan otro efecto de las tecnologías digitales, como el *Health 2.0* o la **atención sanitaria participativa**; los pacientes han comenzado a tomar consciencia y responsabilidad sobre su propia salud a través de su propia investigación sobre lesiones o enfermedades, y la participación en redes sociales donde pueden intercambiar información libremente, y de forma rápida y ágil, y al mismo tiempo ayudarse unos a otros. Se trata de una nueva revolución en salud y tecnología a medida de las personas.

En los fundamentos de esta investigación subyace el enfoque impulsado por el Big Data hacia una **atención sanitaria personalizada** (Blobel, López y González, 2016; Viceconti, Hunter y Hose, 2015; Chawla y Davis, 2013), que defiende su aplicabilidad a resultados centrados en el paciente, con sentido práctico y reducción de las tasas de reingreso. Además de la oportunidad para un creciente **atención preventiva** que ofrece el *eHealth*, uno de los campos con mayor potencial, a través de múltiples dispositivos que los pacientes pueden configurar de forma personalizada. El consumidor y usuario está conectado como nunca, y busca soluciones de salud y bienestar personalizadas.

5.1.8. Necesidad de confianza de los consumidores.

Por todo ello, la educación ciudadana es importante en el contexto de las TIC (Sánchez Rojo, 2016) y del sector salud; como bien apunta Kenny (2016) cuando las personas no conocen los riesgos de la divulgación de datos de salud, o los beneficios de las tecnologías aplicadas a la salud, no es fácil que puedan tomar decisiones informadas; estudios como el suyo han puesto de manifiesto que los ciudadanos en Europa (y EE.UU.) carecen actualmente de una comprensión de cómo sus datos de salud son utilizados por profesionales de la salud y proveedores de tecnología para la salud. Este dato pone de relieve la necesidad de educar a los ciudadanos y mejorar sus conocimientos sobre el uso de la información, especialmente en el contexto de sus datos de salud.

Como defiende Cordero (2016), el nuevo RGPD se posiciona a favor de la certificación como herramienta de prevención y adaptación a los cambios tecnológicos, pero teniendo en cuenta que la actualización de los requisitos técnicos (que constituyen el objeto de certificación) debe realizarse de manera que éstos se acomoden de forma ágil a los constantes cambios tecnológicos, **incorporando aspectos legales al esquema de certificación**, para que el sello o la marca tengan un verdadero valor (al proteger de forma efectiva los derechos de los consumidores y usuarios, y de esta forma contribuir al aumento de la confianza en estos mecanismos). De esta forma, la implementación de nuevos esquemas de certificación en la UE representan una garantía de derechos fundamentales de los consumidores y usuarios, como la protección de los datos de carácter personal, y muy especialmente los de salud.

El volumen de información que se genera cada día es enorme, el Big Data almacena y procesa datos para aportar información que pueda ser útil, según los profesionales de las nuevas tecnologías y en general de la información. Nadie duda de la relevancia del Big Data hoy en día para las empresas, en una carrera por aprovechar la gran cantidad de datos que se generan en todo el mundo para tomar decisiones que puedan favorecer el negocio, **una nueva forma de predecir el futuro,** que puede ayudar en esa toma de decisiones. Para evitar riesgos en la privacidad, algunos autores proponen que la minería de datos, incluyendo las políticas de privacidad en Internet, vayan unidas a un **código de conducta ética** que la regule y que puede tener implicaciones importantes, como la mayor confianza de los consumidores y proveedores de datos (Dean, Payne y Landry, 2016). Se habla del Big Data como el nuevo petróleo del siglo XXI pero en realidad parecen más un **nuevo campo de cultivo**; que necesita nutrientes, elegir el lugar correcto para su desarrollo, alimentar correctamente esas semillas, y respetar el entorno natural. Así, disponer de un número ingente de datos o hacer minería de datos será poco efectivo sin tener un marco teórico que aplicar, y ese marco debe cumplir con el derecho fundamental a la protección de los datos personales especialmente sensibles, como son los de la salud.

En esta analítica predictiva y en el núcleo de los procesos para transformar los datos en información, el individuo se erige como protagonista siempre. Con participación del ser humano o sin ella hablamos ya de **inteligencia artificial**, donde las propias máquinas aprenden y extraen sus conclusiones. La inteligencia artificial ha superado los peores vaticinios, y no sólo ofrece analítica a gran velocidad sino una capacidad real de aprendizaje. Es el Big Data, que se puede considerar abiertamente como contenidos de los que aprender, lo que han contribuido al resurgir de la inteligencia artificial, unido por supuesto a otros factores como la creciente velocidad de computación y a los algoritmos. Así todo, parece que **será la inteligencia artificial la que supere a la actual analítica predictiva**.

La evolución biológica del ser humano es lenta, muy lenta, así nuestro ADN (el software de los humanos) y el de los neandertales son muy similares; sus genomas son idénticos en al menos un 99.5% (Noonan et al., 2006). En cambio la tecnología sí crece a enorme velocidad, por ello se puede hablar de un futuro con seres humanos digitales tal vez y ello me lleva a preguntarme ¿dónde quedará su derecho a la privacidad? En todo caso hay que tener en cuenta que la protección de los datos personales corren el riesgo de obstaculizar o incluso impedir el acceso a los datos personales que pueden contribuir a mejorar nuestra salud, Dyke, Dove y Knoppers (2016) proponen en todo caso respetar los intereses relativos a la privacidad de los particulares cuyos datos se destinen a la investigación del genoma así como en la atención clínica.

Si en el mundo actual, de una lenta evolución biológica (por millones de años), una especie es superior a otra ¿qué sucederá cuando el mundo biológico quede superado en las próximas décadas por la **superinteligencia** (una máquina cuya inteligencia supere al ser humano en todos los ámbitos)? ¿estarán nuestros datos, incluidos los de salud, a buen recaudo? desafíos para el futuro. De acuerdo a la frase atribuida a Julio Verne lo que un hombre es capaz de imaginar, otros lo podrán realizar; se ha especulado sobre si Julio Verne era un visionario, o en realidad si su gran conocimiento de los avances tecnológicos de su época unido a su asombrosa imaginación le condujeron a prever con gran acierto muchos de los logros científico-técnicos que se producirían más tarde (Roy, 2005). Hoy la superinteligencia está muy cerca, y no parece ciencia ficción a la vista de los avances en la inteligencia artificial. ¿Estos avances representarán una evolución del concepto de protección de datos personales, o será más bien una **revolución**?.

La revolución de la investigación sanitaria sólo acaba de empezar; tres hitos parecen marcar los estudios de salud: la detección del ADN mediante la reacción en cadena de la polimerasa -PCR- (1986), la secuenciación del genoma (1999) y la manipulación genética (CRISPR, 2015). El desafío del envejecimiento por ejemplo, nos lleva a la manipulación de los genes y a la privacidad de los datos genéticos; los datos genéticos son especialmente susceptibles de ser utilizados para discriminar a las personas en muchas facetas de su vida; discriminación en función del mapa genético (González, 2011).

En este contexto donde las nuevas tecnologías han entrado de lleno en casi todos los ámbitos de la vida cotidiana, especialmente en el de las relaciones sociales y la salud de los seres humanos, las redes sociales en Internet representan un herramienta muy útil tanto desde el ámbito personal como desde el profesional; llevado al campo de la salud entran en juego tantos factores desde el punto de vista de la protección de los datos de carácter personal, que algunos autores hablan de la virtud de la autorregulación como "estrategia ordenadora idónea de las actividades que se desarrollan en la red" (López, 2009); parece razonable pensar que un futuro habrá siempre más riesgos respecto a la información sobre la salud que introduzcamos en las redes sociales, puesto que tendremos un menor control de su uso y tratamiento.

Un estudio de IBM calcula que el 80% de los datos almacenados mediante Big Data **no se aprovechan o no son útiles para la toma de decisiones[254];** este almacenamiento de datos implica un gasto económico cada vez más significante para las empresas, y el hecho de no poder utilizar cierta información con más de un fin representa un escollo. Mucha información no facilita la utilidad deseada, se trata de la denominada información oscura (llamada Dark Data); esta puede servir como canal para saber qué información se tiene que utilizar y en su caso desechar, para de esta manera transformar los resultados empresariales. Si el Dark Data no se indexa o almacena adecuadamente resultará invisible para los científicos o cualquier otro usuario, corriendo el riesgo de perderse o ser infrautilizados (Heidorn, 2008).

Al mismo tiempo, el concepto de privacidad está evolucionando (cuando menos), al pasar de la sociedad de la información a la automatización del mundo, y nos debería hacer reflexionar si el Big Data no lleva dentro de su propio ADN la posibilidad de contribuir al control de quién utiliza los datos y cómo los utiliza; en el fondo es cuestión de **desarrollar la inteligencia artificial que sea capaz de contribuir a vigilar el acceso y el uso que se hace de los datos**. Esta investigación es por ello sólo una reflexión en el camino, nunca un punto y final.

5.1.9. La tecnología como garante.

La tecnología como garante de la seguridad de la información. Así pues una de las conclusiones derivadas esta investigación consiste en la relevancia que adquiere la tecnología de la información para garantizar la privacidad y la seguridad de los datos personales de salud (Rothstein y Knoppers, 2016); la armonización de normas sobre privacidad debe facilitar en general la investigación internacional (Rothestein, Knoppers y Harrel, 2016) y especialmente la relativa a los biobancos[255]. Un biobanco actúa

[254] El Dark Data, el lado oscuro del Big Data (3 agosto 2016).

[255] Según la ley de Investigación Biomédica (Ley 14/2007 de 3 de Julio) un biobanco es un establecimiento público o privado, sin ánimo de lucro, que acoge una colección de muestras biológicas concebida con fines diagnósticos o de investigación biomédica y organizada como una unidad técnica con criterios de calidad, orden y destino.

como una plataforma que acompaña a la investigación, y que opera como un nexo entre donantes, médicos e investigadores para garantizar un tratamiento (que debe ser seguro y eficaz) de muestras biológicas y sus datos asociados; los biobancos en general facilitan estudios en muy distintas áreas de la investigación biomédica, resultando especialmente relevantes para el desarrollo de una medicina personalizada. Junto a problemas técnicos, los biobancos plantean frecuentemente cuestiones relativas a la privacidad y la seguridad que se deben resolver a medida que los biobancos continúan creciendo en escala y alcance (Heatherly, 2016); los mecanismos de consentimiento actualmente en uso varían, y en algunos casos a los participantes se les ofrecen pocas garantías de privacidad, sin embargo la evolución de la tecnología sí aporta mejoras.

Actualmente casi todas las organizaciones dedicadas a la salud tratan datos personales de una manera o de otra, y cada vez más, en la nube, también en materia de *eHealth*. Esta situación exige un buen modelo de gobierno en tecnología de la información que sólo será integral si se dispone de una norma sobre protección de datos de carácter personal, como puede ser la ISO 27018.

Se están desarrollando nuevos programas y sistemas para permitir a los investigadores llevar a cabo su trabajo con éxito. Así, la interoperabilidad en *eHealth* sólo es posible a través de la tecnología. Proyectos europeos como epSOS han contribuido a la convergencia y al progreso en materias como *eHealth*, gracias a la cooperación entre distintos países, facilitando el acceso a la historia clínica de los pacientes, y trabajando en la buena dirección hacia la sostenibilidad del sistema, incluso a nivel semántico. Proyectos como epSOS prueban que la interoperabilidad en el ámbito *eHealth* es posible, si se ponen los medios tecnológicos y las garantías necesarios.

5.2. Limitaciones.

Existen limitaciones a las que me he enfrentado en el desarrollo de esta investigación, de diversa índole, incluida la etapa final de esta investigación cuando se ha aprobado el texto final del nuevo RGPD que será plenamente aplicable desde el 25 de mayo de 2018. Así pues habrá que atender en el futuro a dicho RGPD y su desarrollo, que debe ser motivo de una profunda investigación independiente. Al cierre de esta investigación, **todavía no se ha producido la incorporación del RGPD a la legislación interna** de la mayor parte de los Estados miembros de la UE, incluida la española; actualmente la Comisión general de Codificación está preparando un anteproyecto de modificación de la LOPD, que elevará al Ministro para después seguir con todos los trámites que señala la Ley del Gobierno para elaborar anteproyectos de ley de cara a su remisión a las Cortes Generales.

Por otro lado, Internet es un entorno cambiante por su propia naturaleza, y la legislación va siempre por detrás, por ello los cambios normativos ocurridos en el transcurso de esta investigación (como la sustitución del principio de "Puerto Seguro" por el nuevo "Escudo de Privacidad") llegarán acompañados de una nueva necesidad de regulación o motivados por decisiones de los tribunales (como el caso Schrems), en muchos casos, como respuesta a brechas de privacidad o a demanda de los propios ciudadanos, como aquí se ha concluido.

Existe una falta de transparencia en esta materia, al tratarse de un ámbito sometido a númerosos riesgos especialmente en materia de ciberseguridad, por lo que esta investigación ha sufrido la dificultad para acceder a otros datos de referencia, más allá de los publicados. Esta investigación ha seguido un riguroso criterio al acudir a fuentes de reconocido prestigio y credibilidad pero merece la pena señalar que no todo aquello que se publica es información que se pueda contrastar en toda su extensión.

La estructura, la fortaleza y la financiación de las instituciones en otras jurisdicciones, fuera del territorio de la UE, representa una limitación importante para poder analizar, en igualdad de condiciones, la capacidad de implantar con éxito un régimen regulatorio de protección de datos de carácter personal, que pueda tener una base sólida e independiente de otros poderes del Estado, que sea garante de los derechos fundamentales, especialmente en una materia especialmente protegida, la información relativa a la salud.

Entre las principales limitaciones identificadas en esta investigación está la brecha digital, que como he indicado hace difícil la armonización de sistemas. Por otro lado nos enfrentamos a valores con intereses contrapuestos en gran medida, la tecnología frente a la ley, la investigación frente a los derechos individuales. Deberemos analizar la evolución de la política en protección de datos UE una vez que entre en vigor el nuevo RGPD, y asimismo observar la influencia que imprime en otras jurisdicciones más allá de la UE, incluida la repercusión futura del "Escudo de Privacidad" en el **intercambio de datos con EE.UU.** aprobado en 2016.

Por último, tal vez se podría lograr una perspectiva más integral de la influencia del modelo europeo, y las diferencias con otras jurisdicciones (especialmente con EE.UU.), ampliando esta investigación a futuro en el contexto del análisis de los efectos de la globalización y de la legislación europea en los sistemas jurídicos asiáticos, o en los sistemas jurídicos de otras naciones que se han enfrentado a presiones para posicionarse a favor de un modelo europeo o un marco jurídico menos rígido como el norteamericano[256].

[256] Kagan, 2007.

5.3. Investigaciones futuras.

El modelo regulatorio europeo se impone a todas las iniciativas que deseen tratar datos de ciudadanos en Europa. Parece en todo caso que se avecinan tiempos con mayor presión sobre el cumplimiento normativo y la governanza de los datos. Esta tesis debe formar parte de un proyecto de investigación más amplio, donde se analice cómo la armonización de las leyes de privacidad contribuye a desarrollar la investigación internacional de los biobancos (Rothstein, 2015); esto se debe a que en la colaboración internacional (en materia de investigación en general, y en el área de salud en particular) el intercambio de datos personales, especialmente en consorcios internacionales, se ha convertido en una parte importante del desarrollo de los biobancos, y de otros métodos modernos de investigación en el área de la salud, pues aumenta el poder estadístico de la investigación, ayuda a identificar situaciones especiales e impide la duplicación de esfuerzos en la investigación. La legislación estadounidense tampoco aborda directamente el intercambio internacional de datos o muestras fuera del acuerdo UE-EE.UU.[257], que sólo se aplica a la recepción de datos por parte de entidades estadounidenses de países de la UE (Harrell y Rothstein, 2016), así pues nuevas investigaciones (y reglas) ayudarían a aclarar las protecciones de privacidad en biobancos, y a determinar la suficiencia de las protecciones actuales, así como su capacidad para facilitar o dificultar las colaboraciones internacionales.

Puesto que vivimos en red, la red digital es la nueva sociedad, donde se comparte todo tipo de información y, por supuesto, aquello que nos importa, los datos de salud. Habrá que atender finalmente a quiénes pueden acceder a esos datos, al uso que los distintos agentes hagan de dichos datos (y cómo puede afectar a la necesaria investigación médica), pero también al uso que los ciudadanos hagan finalmente de las medidas de protección de sus derechos fundamentales en la sociedad de la tranparencia de Han (2013).

Como nos recuerda Castells (2014) la tecnología de comunicaciones digitales “ya es una segunda piel para los jóvenes, mientras que, por otro lado, alimenta los temores y las fantasías de los que siguen gobernando una sociedad que ya apenas comprenden”. Con afirmaciones como esta sólo no puedo estar más de acuerdo; el desarrollo de las redes sociales y tecnológicas van a ser protagonistas de futuras investigaciones sin duda alguna, pues cada día se vive más en el entorno de las redes (donde se comparten intereses e información personal que dejará huella para siempre). Así, convendría abarcar sin duda cuál va a ser el alcance de las redes en materia de salud, y cómo van contribuir al desarrollo de nuevos modelos de negocio, incluido el mundo del deporte y bienestar en general.

De tal forma que, gracias a datos biométricos recogidos con pulseras y otros aparatos de medición, medir objetivos para nuestra salud física ya una realidad. Este es una ejemplo de los miles de sistemas que

[257] Anteriormente “Puerto Seguro”, ahora en vigor el acuerdo de “Escudo de Privacidad”.

están apareciendo con los nuevos avances tecnológicos, y que permiten medir y analizar factores que impactan en nuestra salud. Así mismo, algunos sistemas de salud incluyen recoger y agregar datos de pacientes en los puntos de atención, bien sean hospitales, consultas o clínicas, para su análisis y generación de hipótesis, en función del Big Data de pacientes que muestran síntomas similares. A la vista del llamado atlas del genoma del cáncer o de la investigación del Parkinson por ejemplo, habrá que investigar cómo afectarán estas iniciativas a los interesados (pacientes) en el futuro, especialmente si las compañías de seguros participan en los mismos.

En la marco del Brexit aprobado por los británicos el 23 de junio de 2016, cabe preguntarse si el Reino Unido va a poner en práctica las medidas recogidas por el RGPD, si es que decide aplicar las políticas regulatorias de la UE, ahora que el gobierno británico a decidido "retomar el control de sus leyes". Será interesante investigar cuál va a ser el camino que tomará el Reino Unido en materia de *eHealth* y la política de la UE, si es que sus organizaciones (hospitales, aseguradoras, biobancos, etcétera) desean continuar tratando datos de ciudadanos en territorio de la Unión. A la vista de la nueva regulación europea, convendría abordar la influencia del RGPD a partir del 25 de mayo de 2018 con un Reino Unido fuera de la UE.

Por otro lado, habrá que atender a la posición pueda adoptar EE.UU. frente al endurecimiento de las sanciones por incumplimiento de la normativa comunitaria, que afectan muy directamente a los grandes proveedores de servicios de Internet con origen en EE.UU. Conviene recordar que **gran parte del intercambio comercial entre EE.UU. y Europa depende del intercambio de datos de carácter personal**[258].

Estamos asistiendo a alianzas de empresas para ofrecer servicios de salud, están surgiendo cada nez mayores vínculos entre el sector farmaceútico y tecnológico precisamente en el área de salud. ¿Serán capaces de generar la confianza de los ciudadanos europeos?. En 2016 la farmacútica francesa Sanofi y Google, a través de Verify Life Sciences (antes Google Life Sciences) -filial de Alphabet (matriz del gigante de Internet)- han creado una sociedad conjunta para el desarrollo de soluciones que combinen dispositivos, medicina, software y otros servicios dirigidos a mejorar la calidad de vida de personas con diabetes. Esto es sólo el comienzo.

Se deben abarcar cuestiones cómo los límites del abaratamiento de los costes con la llegada del Big Data al ámbito de la salud; los sistemas sanitarios maduros se enfrentan al reto de velar por la salud de cada

[258] Tal y como ha afirmado de la Comisaria Europea de Justicia, Věra Jourová, respecto al nuevo acuerdo UE-EE.UU relativo al "Escudo de Privacidad" (que regula las transferencia de datos a empresas en EE.UU), y al que ya se han acogido al menos 1.100 compañías. Recuperado de http://www.euractiv.com/section/justice-home-affairs/news/jourova-seeks-data-protection-talks-with-trumps-people-as-soon-as-possible/. Último acceso 20 enero 2017.

vez más ciudadanos, y más envejecidos, a la vez que se aspira a garantizar tratamientos con la mayor calidad al menor coste posible. El Big Data, como se ha analizado en profundidad a lo largo de esta investigación, puede ayudar a médicos y profesionales sanitarios a la hora de tomar mejores y más acertadas decisiones, a detectar riesgos para la salud de los pacientes y prescribir la medicación o tratamientos adecuados, que eviten lo que conocemos (de antemano) va a ocurrir (resultado), a la vez que las grandes bases de datos incluyen historiales de miles de personas que sirven para guiar la posible evolución de nuevos pacientes. Habrá que analizar el acceso a esas bases de datos, incluidas las listas negras, especialmente a la vista del ánimo de lucro de muchas empresas del sector, para determinar si se ajustan o no a la ley, las códigos de conducta, y la normalización.

Como indica Rincón (2016) los ciudadanos como individuos debemos concienciarnos sobre este serio problema que afecta a la intimidad y a la democracia. Habla con razón de abandonar la inocencia, de cliquear "Me gusta", de "estar conectado" y del "placer de exponerse". Apoyar los avances tecnológicos si, pero luchar contra la vigilancia y el control (especialmente de grandes compañías y gobiernos), o no existirá ni intimidad ni democracia real, es decir, respeto a los derechos fundamentales (Rojas, 2016; Delgado 2016). Conviene aquí pues abrir nuevas líneas de investigación, referidas al Derecho Internacional como elemento integrador; es decir, en la complejidad de la sociedad internacional actual y reconocida su personalidad jurídica internacional, analizar el papel de las organizaciones internacionales como entidades con vocación de permanencia (de carácter universal o regional) en las que los Estados cooperan, como bien señala Caballero (2016) en relación al Convenio Europeo de Derechos Humanos como factor de integración en Europa.

Los Estados miembros de la UE han sido hasta ahora los responsables de transponer las Directivas a sus ordenamientos jurídicos (en tiempo y forma), así como de velar por la correcta aplicación y ejecución de la legislación de la UE en general. Pero lo cierto es que en última instancia la futura aplicación e influencia del Derecho de la UE dependerá de las consecuencias del nuevo RGPD en la UE y queda, a mi entender, **a expensas de las denuncias que los propios particulares puedan interponer en defensa de sus derechos** (Pérez, 2015; Delgado, 2016) -tal y como el caso Schrems ha demostrado- y de las medidas que puedan tomar las empresas, dentro y fuera de Europa, desde el punto de vista comercial y de competividad de negocio (Gregorio, 2004; Angarita 2010), y no sólo estará vinculado a la legislación que terceros países puedan llegar a aprobar sobre esta materia.

Se abren así nuevas líneas de investigación, muy interesantes para su estudio, porque la **protección de datos y el cuidado de la salud están en constante evolución, hoy más que nunca, pendientes y dependientes de la tecnología**; se trata de un terreno de juego que va a sufrir una enorme presión tanto de los actores políticos, económicos como de los ciudadanos propiamente dichos, los únicos depositarios de un

derecho inalienable que afecta a su integridad y a la propia vida. Será por ello interesentate atender a futuras investigaciones sobre la aplicación de tecnologías innovadoras a la resolución de problemas, en este caso, determinar si la inteligencia artificial permite, no ya realizar predicciones sobre futuras epidemias, sino definir parámetros de uso y control de acceso a datos de carácter personal.

"En el siglo de la mala educación y las noticias falsas, nada más valioso que un dato, especialmente si es verídico, para superar la crisis de valores".

Alejandro Kress

(Significado de "verídico" según la Real Academia Española - proviene del latín "veridĭcus" -:

1. adj. Que dice verdad.
2. adj. Que incluye la verdad).

Referencias bibliográficas.

Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big data research in information systems: Toward an inclusive research agenda. Journal of the Association for Information Systems, 17(2), 3.

Abugessaisa, I., Saevarsdottir, S., Tsipras, G., Lindblad, S., Sandin, C., Nikamo, P., ... & Tegnér, J. (2014). Accelerating translational research by clinically driven development of an informatics platform–a case study. PloS one, 9(9), e104382.

Adamson, G. (2016). The persistent challenge of health informatics. Information, Communication & Society, 19(4), 551-558.

AENOR (noviembre 2016). Normas en Nuestra Vida. Revista de la normalización y la certificación, (320), 52.

AEPD. El Reglamento de Protección de Datos. Recuperado de https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php. Último acceso 15 enero 2017.

AEPD. Informe Jurídico 0262/2011. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2011-0262_Cesi-oo-n-de-datos-a-Registro-de-c-aa-ncer..pdf. Último acceso 9 enero 2017.

AEPD. Informe Jurídico 0488/2008. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2008-0488_Tratamiento-y-Cesi-oo-n-de-datos-de-salud-con-finalidad-desconocida.pdf. Último acceso 30 diciembre de 2016.

AEPD. Informe Jurídico 0471/2008. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2008-0471_Consentimiento-en-la-recogida-de-datos-de-salud.pdf. Último acceso 8 enero 2017.

AEPD. Informe Jurídico 2000/0000. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2000-0000_Tratamiento-de-datos-gen-ee-ticos-para-la-localizaci-oo-n-de-personas-desaparecidas-o-en-investigaci-oo-n-criminal.pdf. Último acceso 10 diciembre de 2016.

AEPD. Funciones de carácter general. Recuperado de https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/el-director-ides-idphp.php. Último acceso 5 diciembre 2016.

AEPD. Informe Jurídico 1999/0000. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/1999-0000_Naturaleza-de-los-datos-psicol-oo-gicos-a-efectos-de-su-tratamiento.pdf. Último acceso 30 noviembre de 2016.

Agenda Digital para España. Recuperado de http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx. Último acceso 5 enero 2017.

Aggarwal, C. C. (2011). An introduction to social network data analytics. In Social network data analytics (pp. 1-15). Springer US.

Aguilar, L. J. (2016). Big Data, Análisis de grandes volúmenes de datos en organizaciones. Alfaomega Grupo Editor.

Aguilera, A. T. (2001). Nuevas tecnologías, intimidad y protección de datos: con estudio sistemático de la Ley orgánica 15/1999. Edisofer.

Alcalá, H. N. (2016). Dignidad de la persona, derechos fundamentales y bloque constitucional de derechos: una aproximación desde Chile y América Latina. Revista de Derecho, (5).

Alcántara, J. F. (2008). La sociedad de control. Privacidad, propiedad intelectual y el futuro de la libertad. Colección Planta29. El Cobre Ediciones. Barcelona.

Aluja Banet, T. (2001). La minería de datos, entre la estadística y la inteligencia artificial. Qüestiió, Universitat Politècnica de Catalunya, 25(3).

Álvarez, A. Á. (2012). Análisis de la motivación en un contexto 2.0 de trabajo colaborativo. Vivat Academia, (117E), 958-969.

Álvarez Hernando, J. (2011). Guía práctica sobre Protección de Datos: cuestiones y formularios. Lex Nova, Valladolid.

American Medical Association. (23 septiembre 2013). HIPAA: Health Insurance Portability and Accountability Act. Recuperado de http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page. Último acceso 15 marzo 2016.

Análisis de la norma ISO/IEC 27018. Recuperado de http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal. Último acceso 2 enero 2017.

Andreu-Perez, J., Poon, C. C., Merrifield, R. D., Wong, S. T., & Yang, G. Z. (2015). Big data for health. IEEE journal of biomedical and health informatics, 19(4), 1193-1208.

Anduiza, E. (2009). Internet, campañas electorales y ciudadanos: el estado de la cuestión. Quaderns del CAC, 33, 5-12.

Angarita, N. R. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. International Law: Revista Colombiana de Derecho Internacional, 8(16).

Area-Moreira, M., y Ribeiro-Pessoa, M. T. (2012). De lo sólido a lo líquido: las nuevas alfabetizaciones ante los cambios culturales de la Web 2.0. Comunicar: revista científica de comunicación y educación, 19(38), 13-20.

Arellano Toledo, W. (2012). Privacidad y protección de datos en internet: España, la Unión Europea y México. Tenorio Cueto, Guillermo (Coordinador) Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares. México DF Editorial Porrúa-Universidad Panamericana.

Argentina es país pionero en América Latina. Recuperado de http://www.novagob.org/pages/view/207197/proteccion-de-datos-personales-en-argentina. Último acceso 4 diciembre 2016.

Arnold, R., Hillebrand, A., & Waldburger, M. (2015). Personal Data and Privacy. Ofcom. London.

Arteaga, S. (2014). Implicaciones legales de la prestación de servicios de cloud computing. Especial referencia a la protección de datos de carácter personal. Revista da AJURIS, 41(135).

Asri, H., Mousannif, H., Al Moatassime, H., & Noel, T. (2015, June). Big data in healthcare: Challenges and

opportunities. International Conference on Cloud Technologies and Applications (CloudTech), IEEE, 1-7.

Atun, R., De Andrade, L. O. M., Almeida, G., Cotlear, D., Dmytraczenko, T., Frenz, P., ... & De Paula, J. B. (2015). Health-system reform and universal health coverage in Latin America. The Lancet, 385(9974), 1230-1247.

Auffray, C., Balling, R., Barroso, I., Bencze, L., Benson, M., Bergeron, J., ... & Del Signore, S. (2016). Making sense of big data in health research: Towards an EU action plan. Genome medicine, 8(1), 71.

Austin, C., & Kusumoto, F. (2016). The application of Big Data in medicine: current implications and future directions. Journal of Interventional Cardiac Electrophysiology, 1-9.

Baden-Fuller, C., & Haefliger, S. (2013). Business models and technological innovation. Long range planning, 46(6), 419-426.

Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2014). Transformational issues of big data and analytics in networked business. MIS quarterly, 38(2), 629-631.

Baro, E., Degoul, S., Beuscart, R., & Chazard, E. (2015). Toward a literature-driven definition of big data in healthcare. BioMed research international, 2015.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. Privacy, big data, and the public good: Frameworks for Engagement, 44-75.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. Communications of the ACM, 57(11), 31-33.

Bates, D. W. (1997). Commentary: quality, costs, privacy and electronic medical data. JL Med. & Ethics, 25, 111.

Bates, D. W. & Wright, A. (2009). Evaluating eHealth: undertaking robust international cross-cultural eHealth research. PLoS Med, 6(9), e1000105.

Bäumer, U., von Oelffen, S., & Keil, M. (2017). Internet of Things: Legal Implications for Every Business. In The Palgrave Handbook of Managing Continuous Business Transformation (pp. 435-458). Palgrave Macmillan UK.

BBC. Escándalo de Espionaje: qué es el club de los cinco ojos. Recuperado de: http://www.bbc.com/mundo/noticias/2013/10/131030_internacional_estados_unidos_espionaje_reino_unido_club_cinco_ojos_az. Último acceso 3 enero 2017.

BBMRI (Biobanking and Biomolecular Resources Research Infrastructure). Recuperado de https://www.structuralbiology.eu/resources/organisations/bbmri-biobanking-and-biomolecular-resources-research-infrastructure. Último acceso 4 diciembre 2016.

Beck, Ulrich. (2013, 30 agosto). El Riesgo para la libertad. El País. Recuperado de http://elpais.com/elpais/2013/08/14/opinion/1376502906_653929.html.

Beidas, R. S., Marcus, S., Aarons, G. A., Hoagwood, K. E., Schoenwald, S., Evans, A. C., ... & Adams, D. R. (2015). Predictors of community therapists' use of therapy techniques in a large public mental health system. JAMA pediatrics, 169(4), 374-382.

Belt.es. Los datos de tu salud que recopilan los dispositivos, un negocio para las empresas. Recuperado de http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=18211. Último acceso 10 diciembre de 2016.

Bender, D. (2014). Which regime offers more actual privacy – US or EU?, LexisNexis 7189.

Bennett, C. & Raab, C. (2006). The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge. The MIT Press, 8&298.

Benevenuto, F., Rodrigues, T., Cha, M., & Almeida, V. (2009, November). Characterizing user behavior in online social networks. InProceedings of the 9th ACM SIGCOMM conference on Internet measurement conference (pp. 49-62). ACM.

Bernard, E. (2014, May). Supporting diagnosis and treatment in medical care based on big data processing. In Cross-Border Challenges in Informatics with a Focus on Disease Surveillance and Utilising Big Data: Proceedings of the EFMI Special Topic Conference, 27-29 April 2014, Budapest, Hungary (Vol. 197, p. 65). IOS Press.

Bimber, B. (2001). Information and political engagement in America: The search for effects of information technology at the individual level. Political Research Quarterly, 54(1), 53-67.

Birnhack, M. D. (2008). The EU data protection directive: an engine of a global regime. Computer Law & Security Review, 24(6), 508-520.

Boehm, F. (2011). Information sharing and data protection in the area of freedom, security and justice: Towards harmonised data protection principles for information exchange at EU-level. Springer Science & Business Media.

Bollier, D., & Firestone, C. M. (2010). The promise and peril of big data (p. 1). Washington, DC: Aspen Institute, Communications and Society Program.

Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data protection in social networks. In Economics of information security and privacy (pp. 121-167). Springer US.

Boswarthick, D., Elloumi, O., & Hersent, O. (Eds.). (2012). M2M communications: a systems approach. John Wiley & Sons.

Boyer, C., Appel, R. D., Ball, M. J., van Bemmel, J. H., Bergmans, J. P., Carpentier, M., ... & Safran, C. (2016). Health On the Net's 20 Years of Transparent and Reliable Health Information. Studies in health technology and informatics, 228, 700.

Bradford, A. (2012). The Brussels Effect. Northwestern University Law Review, 107(1).

Brynjolfsson, E., & McAfee, A. (2012). Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy. Brynjolfsson and McAfee.

Buisán, L. & Sánchez Urrutia, A. (2011). Intimidad, confidencialidad y protección de los datos de salud. Editorial Aranzadi Thomson Reuters.

Bulger, M., Taylor, G., & Schroeder, R. (2014). Data-Driven Business Models: Challenges and Opportunities of Big Data.. Oxford Internet Institute September.

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford: Oxford University Press.

Bylund, C. L., D'Agostino, T. A., Ostroff, J., Heerdt, A., Li, Y., & Dickler, M. (2012). Exposure to and intention to discuss cancer-related internet information among patients with breast cancer. Journal of

Oncology Practice, 8(1), 40-45.

Bylund, C. L., Gueguen, J. A., Sabee, C. M., Imes, R. S., Li, Y., & Sanford, A. A. (2007). Provider–patient dialogue about Internet health information: an exploration of strategies to improve the provider–patient relationship. Patient education and counseling, 66(3), 346-352.

Caballero, S. S. (2016). El sistema del Convenio Europeo de Derechos Humanos como factor de integración en Europa. Revista Urbe et Ius, 1(14).

Cano, I., Lluch-Ariet, M., Gomez-Cabrero, D., Maier, D., Kalko, S., Cascante, M., ... & Roca, J. (2014). Biomedical research in a digital health framework. Journal of translational medicine, 12(2), 1.

Cañedo Andalia, R. (2011). Los buscadores en la recuperación de información en salud. ACIMED, 22(3), 219-236.

Carneiro, R., Toscano, J. C., & Díaz, T. (2009). Los desafíos de las TIC para el cambio educativo. Fundación Santillana: Madrid.

Castaneda, A. U. (2016). El mercado único digital será la clave del éxito para el comercio internacional en la Unión Europea. Realidad y Reflexión, 42, 39-54.

Castells, M. (2016). ¿ Comunidades virtuales o sociedad red?.

Castells, M. (2014). El impacto de internet en la sociedad: una perspectiva global. C@ mbio, 19.

Castells, M. (2012). Redes de indignación y esperanza: los movimientos sociales en la era de Internet. Alianza Editorial.

Castells, M. (2001). Internet y la sociedad red. La factoría, 14, 15.

Castro, R. P. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible?. InDret, (1).

Centola, D., & Van de Rijt, A. (2015). Choosing your network: Social preferences in an online health community. Social Science & Medicine, 125, 19-31.

Chan, J., & Moses, L. B. (2016). Making Sense of Big Data for Security. British Journal of Criminology, azw059.

Chang, H., & Choi, M. (2016). Big data and healthcare: building an augmented world. Healthcare Informatics Research, 22(3), 153-155.

Chawla, N. V., & Davis, D. A. (2013). Bringing big data to personalized healthcare: a patient-centered framework. Journal of general internal medicine, 28(3), 660-665.

Chesbrough, H. (2013). Open business models: How to thrive in the new innovation landscape. Harvard Business Press.

Cho, J. (2016). The impact of post-adoption beliefs on the continued use of health apps. International journal of medical informatics, 87, 75-83.

Chong, A. (2007). Investor protection and corporate governance: Firm-level evidence across Latin America. Stanford University Press.

Chou, W. Y. S., Hunt, Y. M., Beckjord, E. B., Moser, R. P., & Hesse, B. W. (2009). Social media use in the United States: implications for health communication. Journal of medical Internet research, 11(4).

Claxton, K., Palmer, S., Longworth, L., Bojke, L., Griffin, S., Soares, M., ... & Rothery, C. (2016). A comprehensive algorithm for approval of health technologies with, without, or only in research: The key principles for informing coverage decisions. Value in Health.

Clements, B., Dybczak, K., & Soto, M. (2016). Más viejos y más pequeños: las repercusiones fiscales de la disminución de la población, así como de su envejecimiento, amenazan por igual a las economías avanzadas y las de mercados emergentes. Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y del Banco Mundial, 53(1), 12-15.

Cliquet, G. (Ed.). (2013). Geomarketing: Methods and strategies in spatial marketing. John Wiley & Sons.

Cole, J., Watkins, C., & Kleine, D. (2016). Health advice from Internet discussion forums: how bad is dangerous?. Journal of medical Internet research, 18(1).

Comisión Europea. eHealth Network. Recuperado de: https://ec.europa.eu/health/ehealth/policy/network_es.

Último acceso 23 enero 2017.

Comisión Europea, comunicado al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. ICT Standardisation Priorities for the Digital Single Market. Obtenido de https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market. Último acceso 22 enero 2017.

Comisión Europea. Interoperable eHealth is worth it. Recuperado de http://www.ehr-impact.eu/downloads/documents/ehr_impact_study_final.pdf. Último acceso 9 enero 2017.

Comisión Europea. La Comisión Europea pone en marcha el Escudo de Privacidad UE-EE.UU. Recuperado de http://europa.eu/rapid/press-release_IP-16-2461_es.htm. Último acceso 5 enero 2017.

Comisión Europea. Europa 2020. Recuperado de http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_es.htm. Último acceso 2 enero 2017.

Comisión Europea. "Study on Big Data in Public Health, Telemedicine and Healthcare", 16 diciembre 2016.

Comisión Europea. Data Protection Eurobarometer Factsheet. Recuperado de http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.

Último acceso 12 diciembre 2016.

Comisión Europea. Marché Unique Numérique. Recuperado de http://ec.europa.eu/priorities/digital-single-market/index_fr.htm. Último acceso 1 diciembre 2016.

Comisión Europea (2015). Eurobarómetro especial 431. Protección de datos.

Comisión Europea, MEMO/13/1059 del 27 de noviembre de 2013.

Comisión Europea, MEMO/12/959 del 7 de diciembre de 2012.

Comisión Europea (2012). The 2012 Ageing Report: Economic and budgetary projections for the EU27 Member States (2010-2060). Recuperado de http://ec.europa.eu/economy_finance/publications/european_economy/2012/pdf/ee- 2012-2_en.pdf. Último

acceso 6 diciembre de 2016.

Comisión Europea (2011). Eurobarómetro especial 359. Actitudes sobre protección de datos e identidad electrónica en la Unión Europea.

Consejo de Europa & FRA. Handbook on European Data Protection Law. Recuperado de http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf. Último acceso 13 enero 2017.

Consejo de la UE (11 junio 2015). 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). Recuperado de http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Último acceso 7 diciembre 2015.

Consejo de la UE. Recomendación R (97) 5 del Comité de Ministros a los Estados miembros relativa a la protección de datos médicos.

Consejo de la UE. Recomendación no R (91) 15 del Comité de Ministros a los Estados miembros, en materia de estudios epidemiológicos en el ámbito de la salud mental.

Consejo de la UE. Conclusiones del Consejo sobre la sostenibilidad de las finanzas públicas ante el envejecimiento de la población. Recuperado de http://www.consilium.europa.eu/es/press/press-releases/2015/05/12-ecofin-ageing-populations/. Último acceso el 12 de noviembre de 2016.

Coorevits, P., Sundgren, M., Klein, G. O., Bahr, A., Claerhout, B., Daniel, C., ... & De Moor, G. (2013). Electronic health records: new opportunities for clinical research. Journal of internal medicine, 274(6), 547-560.

Copping, R., & Lee, M. (2016). The Promise and Challenge of Big Data for Pharma. Harvard Business Review.

Cordero, J. A. V. (2016). La implementación de nuevos esquemas de certificación en la UE como garantía de protección de los derechos fundamentales de consumidores y usuarios (especial referencia a la protección de datos personales). Revista CESCO de Derecho de Consumo, (19), 28-40.

Cotlear, D., Gómez-Dantés, O., Knaul, F., Atun, R., Barreto, I. C., Cetrángolo, O., ... & Lozano, R. (2015).

Overcoming social segregation in health care in Latin America. The Lancet, 385(9974), 1248-1259.

Couttolenc, B., & Dmytraczenko, T. (2013). Brazil's primary care strategy. Washington, DC: World Bank.

Craig, T., & Ludloff, M. E. (2011). Privacy and big data. "O'Reilly Media, Inc.".

Cresswell, K. M., Bates, D. W., & Sheikh, A. (2016). Ten key considerations for the successful optimization of large-scale health information technology. Journal of the American Medical Informatics Association, ocw037.

Cresswell, K. M., Coleman, J., Smith, P., Swainson, C., Slee, A., & Sheikh, A. (2016). INNOVATION IN HEALTH INFORMATICS. Journal of Innovation in Health Informatics Vol, 23(2).

Crotty, B. H., & Mostaghimi, A. (2014). Confidentiality in the digital age. BMJ, 348, g2943.

Currie, W. L., & Seddon, J. J. (2014). A cross-national analysis of eHealth in the European Union: Some policy and research directions. Information & Management, 51(6), 783-797.

Da Cunha Lopes, G., & Teresa, M. (2011). Las recientes reformas en materia de protección de datos. Anuario Jurídico y Económico Escurialense, (44), 317-334.

Damiris, N., & Wild, H. (1997). The Internet: A new agora?. In An Ethical Global Information Society (pp. 307-317). Springer US.

Data Protection in China. Recuperado de http://uk.practicallaw.com/4-519-9017. Último acceso el 12 diciembre de 2016.

Data Protection: No Safe Harbour. Recuperado de https://www.ft.com/content/f2ecc7ca-6e65-11e5-aca9-d87542bf8673. Último acceso 2 diciembre 2016.

De Andrade, L. O. M., Pellegrini Filho, A., Solar, O., Rígoli, F., de Salazar, L. M., Serrate, P. C. F., ... & Atun, R. (2015). Social determinants of health, universal health coverage, and sustainable development: case studies from Latin American countries. The Lancet, 385(9975), 1343-1351.

De Haro Ollé, J. J. (2010). Redes sociales para la educación. Madrid: Anaya.

De Marcos, I. D. F. (2012). Breve aproximación a las implicaciones jurídicas y operativas del tratamiento de datos de salud. Gaceta Médica de México, 148, 480-486.

De Miguel Asensio, P. A. (2014). El tratamiento de datos personales por buscadores de Internet tras la sentencia Google Spain del Tribunal de Justicia. La Ley Unión Europea, 2014(17), 5-11.

Dean, M. D., Payne, D. M., & Landry, B. J. (2016). Data Mining: An Ethical Baseline for Online Privacy Policies. Journal of Enterprise Information Management, 29(4).

Del Registro Civil más antigüo que se conoce: el del Templo de Jerusalén. Recuperado de http://www.mundoarchivistico.com/?menu=articulos&id=477. Último acceso 10 diciembre 2016.

Del Villar, R., de Leon, A. D., & Hubert, J. G. (2001). Regulation of Personal Data Protection and of Reporting Agencies: a Comparison of Selected Countries of Latin America, the United States and European Union Countries.Credit Reporting Systems and the International Economy (MIT Press, Cambridge).

Deleuze, G. (2006). Post-scriptum sobre las sociedades de control. Polis. Revista Latinoamericana, (13).

Delgado, R. G. M. (2016). EL SUJETO CONTEMPORÁNEO: DERECHOS HUMANOS Y DEMOCRACIA/Contemporary subject: human rights and democracy. Nómadas, 47(1), 1.

Delgado, L. R. (2014). Vida privada y protección de datos en la Unión Europea. Dykinson.

Delgado, L. R., & Saltor, C. E. (2013). El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente. Editorial Dykinson, SL.

Delgado, L. R., & Sánchez, Y. G. (2008). Biomedicina y protección de datos. Dykinson.

Della, MV. (2001), "What is e-health (2): the death of telemedicine?", Journal of Med Internet Research; Vol. 3, No. 2.

Demertzis, N., Diamantaki, K., Gazi, A., & Sartzetakis, N. (2005). Greek political marketing online: An analysis of parliament members' web sites. Journal of Political Marketing, 4(1), 51-74.

Denmark, F. (2016). Increased out-of-pocket spending in Europe since recession. PharmacoEconomics & Outcomes News, 757, 17-16.

Dereli, T., Coşkun, Y., Kolker, E., Güner, Ö., Ağırbaşlı, M., & Özdemir, V. (2014). Big data and ethics review for health systems research in LMICs: Understanding risk, uncertainty and ignorance—and catching the black swans?. The American Journal of Bioethics, 14(2), 48-50.

Dezalay, Y., & Garth, B. (1995). Merchants of law as moral entrepreneurs: Constructing international justice from the competition for transnational business disputes. Law and Society Review, 27-64.

Díaz Hernández, B., & Álvarez Pérez, A. (2016). Sociedad de la información y el conocimiento: incidencia en el avance informacional en ciencias médicas. Edumecentro, 8(2), 179-193.

Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare Informatics Research, 22(3), 156-163.

Dixon, J., & Scheurell, R. P. (Eds.). (2016). Social welfare in developed market countries. Routledge.

Dixon, J., & Haslam, P. A. (2015). Does the Quality of Investment Protection Affect FDI Flows to Developing Countries? Evidence from Latin America. The World Economy.

DLA Piper (2016). Manual de Protección de Datos.

Dmytraczenko, T., Torres, F. M., & Aten, A. (2015). Universal Health Coverage Policies in Latin America and the Caribbean. Toward Universal Health Coverage and Equity in Latin America and the Caribbean: Evidence from Selected Countries, 53.

Dmytraczenko, T., & Almeida, G. (Eds.). (2015). Toward universal health coverage and equity in Latin America and the Caribbean: evidence from selected countries. World Bank Publications.

Documento de trabajo sobre las listas negras. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_es.pdf. Último acceso 3 noviembre de 2016.

Domínguez, A. G. (2016). VIH y derechos fundamentales: el derecho a la protección de datos personales y el registro obligatorio de los portadores del VIH en España. Derecho y Realidad, 2(19).

Domínguez, E. R. (2016). La Protección Legal de los Datos Personales y el Spam en el Derecho Argentino (Doctoral dissertation).

Domínguez, D. C. (2009). Democracia 2.0: La política se introduce en las redes sociales. Pensar la publicidad: revista internacional de investigaciones publicitarias, 3(2), 31-48.

Drezner, D. W. (2007). All politics is global. Explaining International Regulatory.

Drucker, P. (26 julio 2010). La mejor forma de predecir el futuro es crearlo. Recuperado de http://www.mercado.com.ar/notas/dossier/366011/1-peter-drucker-la-mejor-forma-de-predecir-el-futuro-e%3Cb%3Es%3Cb%3E-cr. Último acceso 25 de diciembre de 2016.

Durán Cardo, A. B., & García Morales, M. J. (2015). La Figura del responsable en el derecho a la protección de datos.

Dwork, C., & Mulligan, D. K. (2013). It's not privacy, and it's not fair. Stanford Law Review Online, 66, 35.

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: A Critical EU Law. Perspective. Forthcoming European Data Protection Law Review (Lexxion).

Effertz, G., Alverson, D. C., Dion, D., Duffy, V., Noon, C., Langell, K.,... & Lowery, C. (2016). Sustaining and Expanding Telehealth: A Survey of Business Models from Selected Prominent US Telehealth Centers. Telemedicine and e-Health.

El Dark Data, el lado oscuro del Big Data (3 agosto 2016). Recuperado de http://blogthinkbig.com/el-dark-data-el-lado-oscuro-del-big-data/. Último acceso 14 noviembre 2016.

El Registro Civil. Recuperado de http://www.euskalnet.net/e-abizenak/verano02/c_genealogia.html. Último acceso 30 diciembre 2016.

Elixir. Recuperado de https://www.elixir-europe.org. Último acceso 10 octubre 2016.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4), 491-497.

Elwyn, G., Seagrove, A., Thorne, K. & Cheung, W. Y. (2005). Ethics and research governance in a

multicentre study: Add 150 days to your study protocol. BMJ 330: 847.

Enserink, M., & Chin, G. (2015). The end of privacy. Science, 347(6221), 490-491.

EpSOS – Proyecto europeo de eSalud. Retrieved from http://www.epsos.eu/espana/preguntas-mas-frecuentes.html#c20602. Last accessed 13 November 2016.

Escandell, J. R. V. (1986). La implantación del registro civil en España (problemas de utilización en estudios demográficos). In Anales de la Universidad de Alicante. Historia contemporánea (No. 5, pp. 87-100). Area de Historia Contemporánea.

Espay, A. J., Bonato, P., Nahab, F. B., Maetzler, W., Dean, J. M., Klucken, J., ... & Reilmann, R. (2016). Technology in Parkinson's disease: Challenges and opportunities. Movement Disorders.

ETSI. Recuperado de http://www.etsi.org/about. Último acceso 17 de diciembre 2016.

Eurobarometer, F. (2014). European citizens' digital health literacy. A report to the European Commission.

European Commission Information Society and Media Directorate-General (2011). Report on the public consultation on eHealth Action Plan 2012-2020.

European Commission (2007) 'The external dimension of the Single Market review', SEC(2007) 1519, 20 November, Brussels: Commission of the European Communities.

European Observatory on Health Systems and Policies. Informe: Cross Border Heatlh Care in Europe. Recuperado de http://www.euro.who.int/__data/assets/pdf_file/0006/108960/E87922.pdf. Último acceso: 6 diciembre de 2016.

Evolución histórica de los sistema de Registro Civil. Recuperado de http://www.monografias.com/trabajos16/evolucion-registro-civil/evolucion-registro-civil.shtml. Último acceso 12 diciembre de 2016).

Excelerate. Recuperado de https://www.elixir-europe.org/excelerate. Último acceso 16 octubre de 2016.

Eysenbach, G. (2008). Medicine 2.0: social networking, collaboration, participation, apomediation, and openness. Journal of medical Internet research, 10(3), e22.

Eysenbach, G. (2001). What is e-health?. Journal of medical Internet research, 3(2), e20.

Faerberg, E. (2016). Building New Business Models For Success Through Competitiveness and Responsibility. 5th Annual EuroMed Conference of the EuroMed Academy of Business. Journal of European Social Policy, 26(3), 1-20.

Fears, R., Brand, H., Frackowiak, R., Pastoret, P. P., Souhami, R., & Thompson, B. (2014). Data protection regulation and the promotion of health research: getting the balance right. QJM, 107(1), 3-5.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review.Journal of biomedical informatics, 46(3), 541-562.

Fernández-Luque, L., & Bau, T. (2015). Health and social media: perfect storm of information. Healthcare informatics research, 21(2), 67-73.

Fernández, C. M., & Recio, M. (2015). UNE-ISO/IEC 27018: privacidad elevada a la nube. AENOR: Revista de la normalización y la certificación, (309), 20-23.

Fernández Ruiz-Gálvez, E. (2014). Intimidad y confidencialidad en la relación clínica.

Fiordelli, M., Diviani, N., & Schulz, P. J. (2013). Mapping mHealth research: a decade of evolution. Journal of medical Internet research, 15(5), e95.

Flores, L. F. B. (2010). Derechos humanos y salud mental en Europa. Norte de Salud mental, 8(36).

Flores Vivar, J. M. (2009). Nuevos modelos de comunicación, perfiles y tendencias en las redes sociales.

Forman, D., & Sierra, M. S. (2016). Cancer in Central and South America: Introduction. Cancer Epidemiology, 44, S3-S10.

Franco, R.M. (2016). Se reúnen las autoridades de protección de datos en Latino América para un panel de discusión histórico. Recuperado de https://iapp.org/news/a/se-reunen-las-autoridades-de-proteccion-de-datos-en-latino-america-para-un-panel-de-discusion-historico/. Último acceso 3 octubre 2016.

Friedrich, B. (2014). Trends in health communication. Journal of Media Psychology.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (2013). Internet and surveillance: The challenges of Web 2.0 and social media (Vol. 16). Routledge.

GA4GH. Creating a Global Alliance to enable responsible sharing of genomic and clinical data. Recuperado de https://genomicsandhealth.org/files/public/White%20Paper%20June%203%20final_0.pdf. Último acceso 10 enero 2017.

Gallagher, R., & Greenwald, G. (2014). How the NSA plans to infect 'millions' of computers with malware. The Intercept, 12.

Galli, J., Oelrich, J., Taussig, M. J., Andreasson, U., Ortega-Paino, E., & Landegren, U. (2015). The Biobanking Analysis Resource Catalogue (BARCdb): a new research tool for the analysis of biobank samples. Nucleic acids research, 43(D1), D1158-D1162.

Garavand, A., Mohseni, M., Asadi, H., Etemadi, M., Moradi-Joo, M., & Moosavi, A. (2016). Factors influencing the adoption of health information technologies: a systematic review. Electronic Physician, 8(8), 2713.

García Cabrera, H. E., Díaz Urteaga, P., Ávila Chávez, D., & Cuzco Ruiz, M. Z. (2015). La Reforma del Sector Salud y los recursos humanos en salud. In Anales de la Facultad de Medicina (Vol. 76, No. SPE, pp. 7-26). UNMSM. Facultad de Medicina.

García Guzman, M.A. (2013). El derecho fundamental a la protección de datos personales en México: análisis desde la influencia del ordenamiento jurídico español.

García Herrero, J. (22 enero 2017). Jorge García (blog). Recuperado de http://jorgegarciaherrero.com. Último acceso 31 enero 2017.

Garrie, D. B., & Wong, R. (2007). The future of consumer web data: a european/us perspective. International Journal of Law and Information Technology, 15(2), 129-152.

Garriga Domínguez, A. (2016). Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua. Dykinson.

Gasiorowski-Denis, E. (2016). Cómo cambiará nuestra vida con Internet de las Cosas. AENOR: Revista de

la normalización y la certificación, (320), 41-45.

Gellman, B. & Dixon, P. (2014, January). Paying out of Pocket to Protect Health Privacy: A New but Complicated HIPAA Option, A Report on the HIPAA Right to Restrict Disclosure.

George, C., Whitehouse, D., & Duquenoy, P. (2013). Assessing legal, ethical and governance challenges in eHealth. In eHealth: Legal, Ethical and Governance Challenges (pp. 3-22). Springer Berlin Heidelberg.

George, C., Whitehouse, D., & Duquenoy, P. (Eds.). (2012). eHealth: legal, ethical and governance challenges. Springer Science & Business Media.

Gertner, J. (2010, December 14). Social Media as Social Index.The New York Times. Recuperado de http://www.nytimes.com/interactive/2010/12/19/magazine/ideas2010.html?_r=1&#Social_Media_as_Social_Index. Último acceso el 30 de diciembre de 2016.

Giacometti-Rojas, L. F. (2013). Innovación tecnológica y desarrollo de ventaja competitiva en la atención a la salud: enfoque conceptual y metodológico. Gerencia y Políticas de Salud, 12(25).

Gibson, R., & Rommele, A. (2008). Political communication: a comparative politics. Comparative Politics, 473-489.

Gibson, R., Ward, S., & Lusoli, W. (2002). The internet and political campaigning: the new medium comes of age?. Representation,39(3), 166-180.

Gill, J., & Singh, S. (2015). Enormous Possibilities in Big Data: Trends and Applications. Asian Journal of Computer Science and Technology, 4(2), 23-26.

Giménez, A. O. (2015). 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, (10), 57-70.

Glüsing J., Poitras L., Rosenbach M., & Stark (October 20, 2013). Fresh Leak on Us Spying: NSA Accessed Mexican President´s Email. Recuperado de http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html. Último acceso el 14 de febrero de 2016.

Gómez Muñoz, R., & Cañabate Pérez, J. (2016). Las transferencias internacionales de datos personales a Estados Unidos de América y la invalidez del régimen del Safe Harbour.

González, S. Á. (2011). Derechos fundamentales y protección de datos genéticos. Librería Editorial Dykinson.

González, M. E. M., Pascual, C. J., & Mora, S. R. R. (2016). CA 2-245: La Aplicación de las Nuevas Tecnologías de la Comunicación e Información. Enfermería Docente, 1(106), 86.

Goyal, A., Bonchi, F., & Lakshmanan, L. V. (2010, February). Learning influence probabilities in social networks. In Proceedings of the third ACM international conference on Web search and data mining (pp. 241-250). ACM.

Gragnolati, M., Lindelow, M., & Couttolenc, B. (2013). Twenty years of health system reform in Brazil: an assessment of the Sistema Único de Saúde. World Bank Publications.

Greenleaf, G. (2016). Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe.

Greenleaf, G. (2015). Global data privacy laws 2015: 109 countries, with european laws now a minority.

Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. JL Inf. & Sci., 23, 4.

Greenleaf, G., & Georges, M. (2014). The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?.

Greenleaf, G. (2013). Global data privacy laws 2013: 99 countries and counting. Privacy Laws & Business International Report, (123), 10-13.

Greenleaf, G. (2013). Kazakhstan Enacts Central Asia's Second Data Privacy Law. Privacy Laws & Business International Report, (124), 23-24.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108. International Data Privacy Law, 2(2), 2011-39.

Greenleaf, G. (2012). Global data privacy laws: 89 countries, and accelerating. Privacy Laws & Business International Report, (115).

Greenleaf, G. (2011). Global data privacy laws: 40 years of acceleration. Privacy Laws & Business International Report, (112), 11-17.

Greenwald, G. (2014). Sin un lugar donde esconderse, Ediciones B, Madrid.

Greenwald, G. (2013). XKeyscore: NSA tool collects' nearly everything a user does on the internet'. The Guardian, 31.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. The Guardian, 6(06), 2013.

Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 7(6), 1-43.

Greenwald, G., MacAskill, E., & Poitras, L. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian, 9(6).

Gregorio, C. (2004). Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina. Transparentar al Estado. La experiencia mexicana de acceso a la información, 304.

Grossman, L. (2010). Person of the year 2010: Mark Zuckerberg. Time Magazine, 15.

Guarino, A. (2014). The Schizophrenic State: Data Protection versus Surveillance in Europe and America. Available at SSRN 2417623.

Guidi, M., Ruiz-Agundez, I., & Canga-Sanchez, I. (2012). Knowledge Mining from the Twitter Social Network: The Case of Barack Obama. In Computational Social Networks (pp. 211-229). Springer London.

Guzmán Rodríguez, H. 2016. Datos personales en Latinoamérica: ¿dónde estamos?. Recuperado de http://www.ismsforum.es/ficheros/descargas/segurilatam001blq1456907052.pdf. Último acceso 2 enero 2017.

Gyarmati, L., & Trinh, T. A. (2012). Measurement Methods of User Behavior in Online Social Networks. In

Computational Social Networks (pp. 157-175). Springer London.

Haluza, D., & Jungwirth, D. (2015). ICT and the future of health care: aspects of health promotion. International journal of medical informatics, 84(1), 48-57.

Hamilton, B. (2013). Impacts of big data. Potential is huge, so are challenges. Health management technology, 34(8), 12.

Han, B. C. (2014). Psicopolítica. Neoliberalismo y nuevas técnicas de poder.

Han, B. C. (2013). La Sociedad de la Transparencia.

Harrell, H. L., & Rothstein, M. A. (2016). Biobanking research and privacy laws in the United States. The Journal of Law, Medicine & Ethics, 44(1), 106-127.

Hatfield, P. T. (2016). The Great Divide: Recent Trends Could Help Bridge the US EU Data Privacy. Seattle Journal for Social Justice, 14(1), 14.

Hauser, A. (1969). Historia social de la literatura y el arte (Vol. 3, pp. 19-21). Guadarrama.

Hawn, C. (2009). Take two aspirin and tweet me in the morning: how Twitter, Facebook, and other social media are reshaping health care. Health affairs, 28(2), 361-368.

Hearnshaw, H. (2004). Comparison of requirements of research ethics committees in 11 European countries for a non-invasive interventional study. BmJ, 328(7432), 140-141.

Heatherly, R. (2016). Privacy and security within biobanking: The role of information technology. The Journal of Law, Medicine & Ethics, 44(1), 156-160.

Heidorn, P. B. (2008). Shedding light on the dark data in the long tail of science. Library Trends, 57(2), 280-299.

Heitmueller, A., Henderson, S., Warburton, W., Elmagarmid, A., & Darzi, A. (2014). Developing public policy to advance the use of big data in health care. Health Affairs, 33(9), 1523-1530.

Hernández, C. F. (2016). El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre

nuevas perspectivas profesionales. Diario La Ley, (8762), 4.

Herveg, J. (2014). Data Protection and the Patient's Right to Safety. European journal of health law, 21(3), 260-270.

Hilbert, M. (2016). Big data for development: a review of promises and challenges. Development Policy Review, 34(1), 135-174.

Hilbert, M., & López, P. (2011). The world's technological capacity to store, communicate, and compute information. science, 332(6025), 60-65.

Hiller, J., McMullen, M. S., Chumney, W. M., & Baumer, D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. BUJ Sci. & Tech. L., 17, 1.

Hoffman, S. (2016). Electronic Health Records and Medical Big Data: Law and Policy (Introduction).

HonCode. Recuperado de http://www.hon.ch/HONcode/Patients/Visitor/visitor.html. Último acceso 1 de enero 2017.

Hood, L., & Price, N. D. (2014). Demystifying disease, democratizing health care. Science translational medicine, 6(225), 225ed5-225ed5.

Hoofnagle, C. J. (2016). Federal Trade Commission Privacy Law and Policy. Cambridge University Press.

Hoofnagle, C. (2006). Interview with Chris Hoofnagle. Recuperado de http://www.habeasdata.org/wp/2006/07/05/Entrevista_Chris_Hoofnagle/. Último acceso 23 noviembre 2016.

Howe, D. (1993). The free on-line dictionary of computing. FOLDOC.

Hoy entra en vigor el reglamento de protección de datos en toda Europa. Recuperado de http://www.expansion.com/juridico/opinion/2016/05/24/5744979ee5fdeacd408b45e2.html. Último acceso 11 noviembre 2016.

Hu, F. (2016). Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press.

Huesch, M. D. (2013). Privacy threats when seeking online health information. JAMA internal medicine, 173(19), 1838-1840.

Iakovidis, I. (1998). Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe.International journal of medical informatics, 52(1), 105-115.

Islam, M. B., & Iannella, R. (2011, September). Privacy by design: Does it matter for social networks?. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (pp. 207-220). Springer Berlin Heidelberg.

ISO. Recuperado de http://www.iso.org/iso/home/about.htm . Último acceso 1 enero 2017.

ISO/IEC 27018:2014. Recuperado de http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498. Último acceso 2 enero 2017.

ISO/IEEE 11073-10418:2014. Recuperado de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61897. Último acceso 2 enero 2017.

Ison, J., Rapacki, K., Ménager, H., Kalaš, M., Rydza, E., Chmura, P., ... & Booth, T. (2015). Tools and data services registry: a community effort to document bioinformatics resources. Nucleic acids research, gkv1116.

Jacoby, W., & Meunier, S. (2010). Europe and the management of globalization. Journal of European Public Policy, 17(3), 299-317.

Janke, A. T., Overbeek, D. L., Kocher, K. E., & Lévy, P. D. (2016). Exploring the potential of predictive analytics and big data in emergency care. Annals of emergency medicine, 67(2), 227-236.

Janssen, D. (2016). The European Commission's influence in supporting health systems: meeting the healthcare needs of an ageing European population.

Joas, R., Casteleyn, L., Biot, P., Kolossa-Gehring, M., Castano, A., Angerer, J., ... & Horvat, M. (2012). Harmonised human biomonitoring in Europe: activities towards an EU HBM framework. International

journal of hygiene and environmental health, 215(2), 172-175.

Johnson, E. (2007). Data Protection Law in the European Union. The Federal Lawyer, 44-48.

Kagan, R. A. (2007). Globalization and legal change: The "Americanization" of European law?. Regulation & Governance, 1(2), 99-120.

Kamal, N., Fels, S., Blackstock, M., & Ho, K. (2012). The ABCs of designing social networks for health behaviour change: The VivoSpace social network. In Advances in Network Analysis and its Applications (pp. 323-348). Springer Berlin Heidelberg.

Kankanady, R & Wells, M (2013): Health Information Governance in a Digital Environment, Hovenga, E. J., & Grain, H. (Eds), (193), Ios Press, 209-230.

Kankanhalli, A., Hahn, J., Tan, S., & Gao, G. (2016). Big data and analytics in healthcare: Introduction to the special section. Information Systems Frontiers, 18(2), 233-235.

Kaplan, G., G. Bo-Linn, P. Carayon, P. Pronovost, W. Rouse, P. Reid, & R. Saunders. 2013. Bringing a systems approach to health. Discussion Paper, Institute of Medicine and National Academy of Engineering, Washington, DC. Recuperado de http://www.iom.edu/systemsapproaches. Último acceso 20 diciembre de 2016.

Karinthy, F. (1929). Chains. Everything is different, Budapest.

Kawamura, E., & Ronconi, L. (2015). Firms' Investment and Savings in Latin America: Stylized Facts from the Enterprise Survey.

Kelemen, R. D. (2006). Suing for Europe adversarial legalism and European governance. Comparative Political Studies, 39(1), 101-127.

Kelemen, R. D., & Sibbitt, E. C. (2004). The globalization of American law. International Organization, 58(01), 103-136.

Kenny, G. (2016). 'To protect my health, or to protect my health data?'Eexamining the influence of health information privacy concerns on citizens' health technology adoption (Doctoral dissertation, Dublin City University).

Khan, I. U., & ur Rehman, S. (2017). A Review on Big Data Security and Privacy in Healthcare Applications. In Big Data Management (pp. 71-89). Springer International Publishing.

Kim, Y. (2016). Trust in health information websites: A systematic literature review on the antecedents of trust. Health informatics journal, 22(2), 355-369.

Kimble, C. (2015). Business Models for E-Health: Evidence From Ten Case Studies. Global Business and Organizational Excellence, 34(4), 18-30.

Kitchin, R. (2013). Big data and human geography Opportunities, challenges and risks. Dialogues in human geography, 3(3), 262-267.

Knoppers, B. M. (2005). Biobanking: international norms. The Journal of Law, Medicine & Ethics, 33(1), 7-14.

Köppe, E., Bartholmai, M., Daum, W., Gong, X., Holmann, D., Basedau, F., ... & Beck, U. (2016). New Self-diagnostic Fiber Optical Sensor Technique for Structural Health Monitoring. Materials Today: Proceedings, 3(4), 1009-1013.

Korn Ferry Global Study (2016, 17 noviembre). Majority of CEOs See More Value in Technology Than Their Workforce. Recuperado de http://www.kornferry.com/press/korn-ferry-global-study-majority-of-ceos-see-more-value-in-technology-than-their-workforce/. Último acceso 30 noviembre 2016.

Koutkias, V. G., & Jaulent, M. C. (2015). Computational approaches for pharmacovigilance signal detection: toward integrated and semantically-enriched frameworks. Drug safety, 38(3), 219-232.

Kress, A., Monguet, J. M., Navarro, E., & Moreno Reyes, F. (2015). El gran hermano digital monitoriza nuestros datos de salud. Unión Europea Aranzadi, (10), 29-55.

Kress, M. (1986). Normalización y Protección de los consumidores. UNE: Boletín de la Normalización Española, IX(1), 5-9.

Kruse, C. S., Kothman, K., Anerobi, K., & Abanaka, L. (2016). Adoption Factors of the Electronic Health Record: A Systematic Review. JMIR medical informatics, 4(2), e19.

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2012). The challenge of 'big data'for data protection. International Data Privacy Law, 2(2), 47-49.

Kwan, M. P. (2016). Algorithmic geographies: Big data, algorithmic uncertainty, and the production of geographic knowledge. Annals of the American Association of Geographers, 106(2), 274-282.

Kwok, L., & Yu, B. (2013). Spreading social media messages on facebook an analysis of restaurant business-to-consumer communications. Cornell Hospitality Quarterly, 54(1), 84-94.

Labonté, R., & Stuckler, D. (2016). The rise of neoliberalism: how bad economics imperils health and what to do about it. Journal of epidemiology and community health, 70(3), 312-318.

Lara Cicuéndez, M. C. (2015). Información y Privacidad. Delimitación de la Protección General de los Derechos de la Personalidad frente al Derecho a la Información a través del caso de Telma Ortiz Rocasolano.

Las leyes de protección de datos. Recuperado de http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14338%2526ISID%253D507%2526PRT%253D14331,00.html. Último acceso 2 octubre de 2016.

Laurant, C. (15 septiembre 2011). Emerging Data Protection Laws in Latin America and Doing Business in the E.U. Cedric´s privacy blog. Recuperado de https://cedriclaurant.wordpress.com/tag/uruguay/. Último acceso 5 enero de 2017.

Lavenex, S. (2014). The power of functionalist extension: how EU rules travel. Journal of European Public Policy, 21(6), 885-903.

Legge, D. G. (2016). WHO Reform.

Lema Tomé, M. (2014). La reforma sanitaria en España: Especial referencia a la población inmigrante en situación administrativa irregular. EUNOMÍA. Revista en Cultura de la Legalidad, 95-115.

León Sanz, P. (2008). La ética en la práctica. Cuando algo se hace mal: del error médico a la mala praxis. Trauma (Mapfre), 19(3), 138-142.

Lévy, P. (2010). From social computing to reflexive collective intelligence: The IEML research program.

Information Sciences, 180(1), 71-94.

Lévy, P. (2004). Inteligencia Colectiva. Por una antropología del Ciberespacio. Recuperado de http://inteligenciacolectiva.bvsalud.org.

Li, T. (2015). Greenleaf's "Asian Data Privacy Laws": A Key Resource for US And International Privacy Scholars. Georgetown Journal of International Law.

Linares Vallejo, G. (2016). La analítica de Big Data en el sector sanitario.

Lindén, F. (2009). epsos, smart open services for European patients from strategies to services health as the enabler for cross-border healthcare. Infrastructures for Health Care, 23.

Lipton, E., & Hakim, D. (2013). Lobbying bonanza as firms try to influence European Union. New York Times, 18, A1.

Low-Beer, D., & Stoneburner, R. L. (2004). AIDS communications through social networks: catalyst for behaviour changes in Uganda. African Journal of AIDS Research, 3(1), 1-13.

Logan, G. M., & Adams, R. M. (2016). More: Utopia.

López Jiménez, D. (2009). La protección de datos personales en el ámbito de las redes sociales electrónicas: el valor de la autorregulación. Anuario de la Facultad de Derecho (Universidad de Alcalá), (2), 237-274.

Los Angeles Times. FTC in talks with Apple about health data protection. Recuperado de http://www.latimes.com/business/technology/la-fi-tn-ftc-apple-health-privacy-20141114-story.html. Último acceso 10 de diciembre de 2016.

Lundby, K. (2009). Mediatization: concept, changes, consequences. Peter Lang.

Lupiáñez-Villanueva, F., Hardey, M., Torrent, J., & Ficapal, P. (2010). The integration of Information and Communication Technology into medical practice. International journal of medical informatics, 79(7), 478-491.

Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth data security: The need for HIPAA-compliant standardization. Telemedicine and e-Health, 18(4), 284-288.

Lynskey, O. (2014). Deconstructing Data Protection: The 'Added-Value'of a Right to Data Protection in the EU Legal Order. International and Comparative Law Quarterly, 63(03), 569-597.

Llanos, C., & Troncoso, M. (2016). MOVIMIENTOS SOCIALES: CLAVES Y PROPUESTAS DEL TRABAJO SOCIAL. Rumbos TS. Un espacio crítico para la reflexión en Ciencias Sociales, (4), 143-149.

Lloyd, Ian J. (2014). Information Technology Law, 7a edición, Oxford University Press, Oxford.

Machado, S. M. (2015). Los tres niveles de garantías de los derechos fundamentales en la Unión Europea: problemas de articulación. Revista de Derecho Comunitario Europeo, (50), 195-230.

Machado, S. M. (2000). La regulación de la red: poder y derecho en Internet. Taurus Ediciones.

Machanavajjhala, A., & Reiter, J. P. (2012). Big privacy: protecting confidentiality in big data. XRDS: Crossroads, The ACM Magazine for Students, 19(1), 20-23.

Magazine, T. (2006). Time's person of the year: You. US Edition, 168(26).

Mandl, K. D., & Kohane, I. S. (2016). Time for a patient-driven health information economy?. New England Journal of Medicine, 374(3), 205-208.

Manning, A. (2015). Data Protection, Security, and Privacy Policy. In Databases for Small Business (pp. 123-130). Apress.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity. The McKinsey Global Institute.

Manzini, J. L. (2015). Fundamentación bioética de la llamada "adecuación del esfuerzo terapéutico" en el final de la vida. Boletín del Consejo Académico de Ética en Medicina, 9(3).

Mañas, J. L. P., Caro, M. Á., & Gayo, M. R. (2016). Reglamento general de protección de datos: un nuevo modelo europeo de protección de datos.

Mañas, J. L. P. (2009). Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Documentos de trabajo (Laboratorio de alternativas), (147), 1.

Márquez, F. P. G., & Lev, B. (2016). Big Data Management.

Martin, A. B., Hartman, M., Benson, J., Catlin, A., & National Health Expenditure Accounts Team. (2016). National health spending in 2014: faster growth driven by coverage expansion and prescription drug spending. Health Affairs, 35(1), 150-160.

Martin, A. B., Hartman, M., Whittle, L., Catlin, A., & National Health Expenditure Accounts Team. (2014). National health spending in 2012: rate of health spending growth remained low for the fourth consecutive year. Health Affairs, 33(1), 67-77.

Martínez, C. C. (2016). La historia clínica. Aspectos jurídicos y dilemas en el derecho español y colombiano. Via Inveniendi Et Iudicandi, 10(2).

Martínez, R. M. (2016). El Reglamento de protección de datos de la Unión Europea: un reto colectivo. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 25(120), 90-92.

Martínez, R. M. (2014). Privacidad, Estados Unidos y España. Tan lejos, tan cerca. Telos: Cuadernos de comunicación e innovación, (97), 48-56.

Martínez, M. P. N. (2014). Portales sanitarios: propuesta de herramienta de evaluación. Cuadernos de Gestión de Información, 4, 124-138.

Martínez, R. M. (2007). El derecho fundamental a la protección de datos: perspectivas. IDP: revista de Internet, derecho y política= revista d'Internet, dret i política, (5), 4.

Marx, G. T. (2016). Windows into the soul: Surveillance and society in an age of high technology. University of Chicago Press.

Marx, V. (2013). Biology: The big challenges of big data. Nature, 498(7453), 255-260.

Masters, K. (2008). For what purpose and reasons do doctors use the Internet: a systematic review. international journal of medical informatics, 77(1), 4-16.

Mathers, C.D., Stevens, G.A., Boerma, T., White, R.A., & Tobias, M.I. (2015). Causes of international increases in older age life expectancy. The Lancet, 385 (9967), 540-548. doi:10.1016/S0140-

6736(14)60569-9.

Mayer, M. Á., & Leis, Á. (2010). Concepto y aplicaciones de la Web 3.0: una introducción para médicos. Atención primaria, 42(5), 292-296.

Mayer-Schönberger, V. (2016). Big Data for cardiology: novel discovery?. European heart journal, 37(12), 996-1001.

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Mayer Pujadas, M. Á. (2006). Evaluación de los sistemas de acreditación de webs sanitarias: la experiencia de Web Médica Acreditada.

McAfee, A., & Brynjolfsson, E. (2012). Big data. The management revolution. Harvard Business Review, 90(10), 61-67.

McAfee, A., & Brynjolfsson, E. (2008). Investing in the IT that makes a competitive difference. Harvard Business Review, 86(7/8), 98.

McGregor, C. (2013, June). Wearable monitors on babies: Big data saving little people. In Technology and Society (ISTAS), 2013 IEEE International Symposium on (pp. 203-203). IEEE.

McNab, C. (2009). What social media offers to health professionals and citizens. Bulletin of the world health organization, 87(8), 566-566.

Medina-Mora, M. E., Real, T., Villatoro, J., & Natera, G. (2013). Las drogas y la salud pública:¿ hacia dónde vamos?. salud pública de México, 55(1), 67-73.

Meldolesi, E., Van Soest, J., Damiani, A., Dekker, A., Alitto, A. R., Campitelli, M., ... & Lambin, P. (2016). Standardized data collection to build prediction models in oncology: a prototype for rectal cancer. Future Oncology, 12(1), 119-136.

Mendoza, O. F. (2013). El Derecho de cancelación de datos personales en archivos privados en México y España. Derecom, (13), 2.

Meyer, M. (2016). Is Financial Literacy a Determinant of Health?. The Patient-Patient-Centered Outcomes Research, 1-7.

Miguel, C. R. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. Revista de Derecho Comunitario Europeo, 7(14), 7-43.

Milgram, S. (1967). The small world problem. Psychology today,2(1), 60-67.

Miller, A. R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. Management Science, 55(7), 1077-1093.

Minero Alejandre, G. (2014). A vueltas con el "derecho al olvido": Construcción normativa y jurisprudencia del derecho de protección de datos de carácter personal en el entorno digital. Revista Jurídica.

Mitchell, J. (2000). Increasing the cost-effectiveness of telemedicine by embracing e-health. Journal of telemedicine and telecare, 6(suppl 1), 16-19.

Moen, A., Hackl, W. O., Hofdijk, J., Van Gemert-Pijnen, L., Ammenwerth, E., Nykänen, P., & Hoerbst, A. (2012). eHealth in Europe: status and challenges. Eur J Biomed Inform, 8(1), 2-7.

Monleón-Getino, A. (2015). El impacto del Big-data en la Sociedad de la Información. Significado y utilidad/Big-data, a digital ocean in the Information Society. Historia y Comunicación Social, 20(2), 427.

Monteith, S., Glenn, T., Geddes, J., Whybrow, P. C., & Bauer, M. (2016). Big data for bipolar disorder. International journal of bipolar disorders, 4(1), 1.

Monteith, S., Glenn, T., Geddes, J., & Bauer, M. (2015). Big data are coming to psychiatry: a general introduction. International journal of bipolar disorders, 3(1), 1.

Moore, K. L., Persaud, T. V. N., & Torchia, M. G. (2015). The developing human: clinically oriented embryology. Elsevier Health Sciences.

Moore, A. D. (2010, September). Privacy, Public Health, and Controlling Medical Information. In HEC forum (Vol. 22, No. 3, pp. 225-240). Springer Netherlands.

Moreno, J. P. (2014). Una Aproximación a Big Data/An Approach to Big Data1. Revista de Derecho UNED, (14), 471.

Moreno, L. R. M. (2016). Bill Gates. Los negocios en la era digital. región y sociedad, 12(20).

Moreno Reyes, F., Puelles Gayo, M., & Kress, A. (2017). The online social networks as political communication. Journal of Marketing Trends, 4(1), 53-66.

Moreno Reyes, F. (2015). Las redes sociales en Internet como herramienta de estimación del voto.

Moulia, T., Jean, P., y Vilá Costa, B. (2016). La revolución digital, las reglas clásicas sobre protección de datos personales y los flujos transfronterizos.

Mylona, I. (2008). SMS in everyday political marketing in Greece. Journal of Political Marketing, 7(3-4), 278-294.

Naciones Unidas, 2014. La situación demográfica en el mundo, 2014. Informe Conciso. Departamento de Asuntos Económicos y Sociales. División de Población. Nueva York).

Navarro Ruvalcaba, M. A. (2006). Modelos y regímenes de bienestar social en una perspectiva comparativa: Europa, Estados Unidos y América Latina. Desacatos, (21), 109-134.

Navas Navarro, S. (2015). Computación en la nube: Big Data y protección de datos personales (Cloud Computing: Big Data and Personal Data Protection).

Nielsen, P., & Sæbø, J. I. (2016). Three Strategies for Functional Architecting: Cases from the Health Systems of Developing Countries. Information Technology for Development, 22(1), 134-151.

Nilsen, W. (2015). The Use of Technology to Enhance Health. Journal of general internal medicine, 30(8), 1047-1048.

Noonan, J. P., Coop, G., Kudaravalli, S., Smith, D., Krause, J., Alessi, J., ... & Rubin, E. M. (2006). Sequencing and analysis of Neanderthal genomic DNA. science, 314(5802), 1113-1118.

Novella, A. C. (2015). Informe Obimid.

NSA Prism program taps into user data of Apple, Google and others (2013, June 7). The Guardian. Recuperado de https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Último acceso 2 enero 2017.

Nuffield Council on Bioethics (febrero, 2015). Informe: "El almacenamiento, vinculación y uso de los datos en la investigación biomédica y la atención de la salud: cuestiones éticas.

Nunes, A., Santana, C., Bezerra, F., & Sobral, N. (2014). Knowledge Acquisition Based on Geomarketing Information for Decision Making: A Case Study on a Food Company. International Journal of Innovation, Management and Technology, 5(6), 422.

O'Brien, K. (2012). How McDonald's came back bigger than ever New York Times. Retrieved from http://www. nytimes. com/2012/05/06/magazine/how-McDonald's-came-back-bigger-than-ever. html. Last accessed 25 november 2016.

Ohlhorst, F. J. (2012). Big data analytics: turning big data into big money. John Wiley & Sons.

OMS. eHealth. Recuperado de http://www.who.int/topics/ehealth/en/. Último acceso 10 diciembre de 2016.

OMS. The Health Data Ecosystem. Recuperado de http://www.who.int/ehealth/resources/ecosystem/en/. Último acceso 10 diciembre de 2016.

OMS. Global Observatory for eHealth series (2012). Legal frameworks for eHealth.

OMS. Survey 2009 Figures. Recuperado de http://www.who.int/goe/survey/2009/figures/en/index2.html. Último acceso el 10 diciembe de 2016.

Onetti, A., Zucchella, A., Jones, M. V., & McDougall-Covin, P. P. (2012). Internationalization, innovation and entrepreneurship: business models for new technology-based firms. Journal of Management & Governance, 16(3), 337-368.

Organisation for Economic Co-operation and Development (OECD). (2011). How's Life? Measuring Well-being. OECD Publishing, Paris.

Orwell, G. (1990). Nineteen Eighty-Four. 1949. The Complete Works of George Orwell. Ed. Peter Davison, 9, 1986-87.

Osborne Clarke (2012), informe: “La fiebre del oro de los datos”.

Özdemir, V., Badr, K. F., Dove, E. S., Endrenyi, L., Geraci, C. J., Hotez, P. J., ... & Sabra, R. (2013). Crowd-funded micro-grants for genomics and “big data”: an actionable idea connecting small (artisan) science, infrastructure science, and citizen philanthropy. Omics: a journal of integrative biology, 17(4), 161-172.

Palladino, R., Lee, J. T., Hone, T., Filippidis, F. T., & Millett, C. (2016). The great recession and increased cost sharing in european health systems. Health Affairs, 35(7), 1204-1213.

Papacharissi, Z. (2010). Privacy as a luxury commodity. First Monday, 15(8).

Papacharissi, Z. (2010). A private sphere: Democracy in a digital age. Polity.

Parikh, S. V., & Huniewicz, P. (2015). E-health: an overview of the uses of the Internet, social media, apps, and websites for mood disorders. Current opinion in psychiatry, 28(1), 13-17.

Park, R. W. (2016). HW 04-1 Usefulness of Big Data in Clinical Research. Journal of hypertension, 34, e539.

Parlamento Europeo. Resolución del Parlamento Europeo, 29 de octubre de 2015. Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//ES. Último acceso 24 diciembre 2016.

Pérez, S. G., & Domínguez, R. L. (2016). Impacto de las sociedades del conocimiento en la educación/Impact of knowledge societies in education. RICEA Revista Iberoamericana de Contaduría, Economía y Administración, 5(10).

Pérez Morera, E. (2016). Estudio de Soluciones de Seguridad para Apps Móviles en Sanidad.

Person of the Year. Recuperado de http://time.com/3627996/david-ho-person-of-the-year/. Último acceso el 13 de diciembre de 2016.

Peters, C., Blohm, I., & Leimeister, J. M. (2015). Anatomy of Successful Business Models for Complex Services: Insights from the Telemedicine Field.Journal of Management Information Systems, 32(3), 75-104.

Pérez-Molina, J. A., Álvarez-Martínez, M. J., & Molina, I. (2016). La atención médica a los refugiados: una cuestión ética y de salud pública. Enfermedades Infecciosas y Microbiología Clínica, 34(2), 79-82.

Personalized medicine. Recuperado de http://www.p-medicine.eu. Último acceso 15 noviembre de 2016.

Ploem, M. C., Essink-Bot, M. L., & Stronks, K. (2013). Proposed EU data protection regulation is a threat to medical research. BMJ, 346, f3534.

Ploem, M. C. (2006). Towards an appropriate privacy regime for medical data research. European journal of health law, 13(1), 41-63.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. Tex. L. Rev., 93, 85.

Percival, J., & McGregor, C. (2016). An Evaluation of Understandability of Patient Journey Models in Mental Health. JMIR Human Factors, 3(2).

Pérez, A. L. (2015). La aplicación del derecho de la Unión Europea durante 2014 según el informe de la Comisión Europea. Unión Europea Aranzadi, (10), 73-80.

Pérez-Cebollada, E., Martínez-Ruiz, I., & Bernal-Agustín, J. L. (2014). Challenges of M2M Technologies for eHealth. In Future Information Technology (pp. 249-253). Springer Berlin Heidelberg.

Pratt, M., & Franklin, N. C. (2016). Technology and Public Health: New Tools and Perspectives. Progress in cardiovascular diseases, 58(6), 674-675.

Press, G. (2014). Big Data definitions: what's yours. Forbes Tech News.

Protección de datos en Argentina. Recuperado de http://www.novagob.org/pages/view/207197/proteccion-de-datos-personales-en-argentina. Último acceso 4 Deciembre 2016.

Proyecto epSOS. Recuperado de http://www.diariomedico.com/2012/12/26/area-profesional/gestion/proyecto-epsos-espana-es-lider-europeo-tic-salud. Último acceso 12 diciembre de 2016.

Qué es un código tipo en protección de datos. Recuperado de

http://ayudaleyprotecciondatos.es/2010/09/07/que-es-un-codigo-tipo-en-proteccion-de-datos/. Último acceso el 8 de diciembre de 2016.

¿Qué es Big Data?. Recuperado de https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/. Último acceso 23 octubre 2016.

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health Information Science and Systems, 2(1), 1.

Ragnedda, M., & Muschert, G. W. (2013). The digital divide: The Internet and social inequality in international perspective (Vol. 73). Routledge.

Ram, S., Zhang, W., Williams, M., & Pengetnze, Y. (2015). Predicting asthma-related emergency department visits using big data. IEEE journal of biomedical and health informatics, 19(4), 1216-1223.

Ramiro, M. A. (2008). La protección de datos personales en los países de la Unión Europea. Revista jurídica de Castilla y León, (16), 113-168.

Ramiro, M. A. (2006). El derecho fundamental a la protección de datos personales en Europa, Tirant Lo Blanch.

Ramonet, I. (2016). Google lo sabe todo de ti. Le Monde diplomatique en español, (244), 1-2.

Ranallo, P. A., Kilbourne, A. M., Whatley, A. S., & Pincus, H. A. (2016). Behavioral Health Information Technology: From Chaos To Clarity. Health Affairs, 35(6), 1106-1113.

Rao, K. D., Petrosyan, V., Araujo, E. C., & McIntyre, D. (2014). Progress towards universal health coverage in BRICS: translating economic growth into better health. Bulletin of the World Health Organization, 92(6), 429-435.

Rauer, U. (2012). Patient Trust in Internet based Health Records: An Analysis Across Operator Types and Levels of Patient Involvement in Germany. Policy & Internet, 4(2), 1-42.

Read, P., Shah, C., Lupita, S., & Woolcott, J. (2012). 'Story of one's life and a tree of friends'–understanding millennials' information behaviour in social networks. Journal of Information Science, 38(5), 489-497.

Rechel, B., Doyle, Y., Grundy, E., & McKee, M. (2009). How can health sytems respond to population ageing?. European Observatory on Health Systems and Policies, Policy Brief 10.

Regmi, K., Bendel, N., & Gee, I. (2016). Public Health Intelligence: An Overview. In Public Health Intelligence (pp. 1-18). Springer International Publishing.

Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. Stanford Law Review, 1315-1371.

Representación de España ante la UE. Recuperado de http://www.exteriores.gob.es/RepresentacionesPermanentes/EspanaUE/es/quees2/Paginas/El-Derecho-comunitario.aspx. Último acceso el 30 diciembre de 2016.

Representación de España ante Naciones Unidas y Organismos Internacionales. Recuperado de http://www.exteriores.gob.es/RepresentacionesPermanentes/OficinadelasNacionesUnidas/es/quees2/Paginas/Organismos%20Especializados/OMS.aspx. Último acceso el 27 de diciembre de 2016.

Restrepo-Méndez, M. C., Barros, A. J., Requejo, J., Durán, P., Serpa, L. A. D. F., França, G. V., ... & Victora, C. G. (2015). Progress in reducing inequalities in reproductive, maternal, newborn,'and child health in Latin America and the Caribbean: an unfinished agenda. Revista Panamericana de Salud Pública, 38(1), 09-16.

Reuters. U.S. FTC asking Apple about health data protection. Recuperado de http://www.reuters.com/article/us-apple-ftc-exclusive-idUSKCN0IX2I520141113. Último acceso 10 de diciembre de 2016.

RGDP. Recuperado de https://iapp.org/news/a/el-rgpd-el-nuevo-reglamento-europeo-sobre-la-proteccion-de-datos-personales-basado-en-el-principio-de-accountability/. Último acceso 2 enero 2017.

Rich, R. F., & Merrick, K. R. (2006). Cross border health care in the European union: challenges and opportunities. J. Contemp. Health L. & Pol'y, 23, 64.

Richards, N. M., & King, J. H. (2014). Big data ethics. Wake Forest L. Rev., 49, 393.

Rigaux, F. (1990). La protection de la vie privée et des autres biens de la personnalité, Bruxelles: Bruylant.

Rincón, O. (2016). Los datos: la cancha donde se juega la democracia. Chasqui. Revista Latinoamericana de Comunicación, (131), 21-35.

Rincón, A. C. G. (2013). Tenorio Cueto, Guillermo A.(coord.), Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares, México, Porrúa-UP, 2012, 258 pp. Cuestiones Constitucionales, (28), 391-406.

Robles, M. C., Ramírez, M. S. M., Rodríguez, M. M., González, J. M., & Gayo, M. R. (2014). La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo.

Rodrigues, R. J., & Risk, A. (2003). eHealth in Latin America and the Caribbean: development and policy issues. J Med Internet Res, 5(1), e4.

Rodrigues, R. J., Wilson, P., & Schanz, S. J. (2001). The Regulation of Privacy and Data Protection in the Use of Electronic Health Information. Pan American Health Organization: Greenville.

Rodríguez-Iglesias, A., Rodríguez González, A., Irvine, A. G., Sesma, A., Urban, M., Hammond-Kosack, K. E., & Wilkinson, M. D. (2016). Publishing FAIR Data: an exemplar methodology utilizing PHI-base. Frontiers in Plant Science, 7, 641.

Rodríguez, P. E. (2016). Episteme Posmoderna y Sociedades de control: Deleuze, Heredero de Foucault. Revista Margens Interdisciplinar, 6(7), 23-40.

Rodríguez Camiño, R. (2003). Motores de búsqueda sobre salud en Internet. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000500002. Último acceso 10 noviembre de 2016.

Rojas, C. N. (2016). Los derechos fundamentales: debates actuales y desafíos futuros. Revista de Derecho Público, (67), Págs-73.

Rothstein, M. A., & Knoppers, B. M. (2016). Harmonizing Privacy Laws to enable international biobank reaearch: Privacy and Security within Biobanking: The Role of Information Technology. JL Med. & Ethics, 44, 156-216.

Rothstein, M. A., Knoppers, B. M., & Harrell, H. L. (2016). Comparative approaches to biobanks and

privacy. The Journal of Law, Medicine & Ethics, 44(1), 161-172.

Rothstein, M. A. (2016). The end of the HIPAA privacy rule? Currents in contemporary bioethics. The Journal of Law, Medicine & Ethics, 44(2), 352-358.

Rothstein, M. A. (2015). International Health Research after Schrems v. Data Protection Commissioner. Hastings Center Report.

Roy, N. R. (2005). Ciencia y tecnología en la obra de Julio Verne. Matematicalia: revista digital de divulgación matemática de la Real Sociedad Matemática Española, 1(4), 11.

Rubinstein, I. S. (2013). Big data: the end of privacy or a new beginning?. International Data Privacy Law, 3(2), 74-87.

Rumsfeld, J. S., Joynt, K. E., & Maddox, T. M. (2016). Big data analytics to improve cardiovascular care: promise and challenges. Nature Reviews Cardiology.

Rusia bloqueó hoy la red profesional LinkedIn de Microsoft. Recuperado de http://www.elmundo.es/tecnologia/2016/11/17/582d7f44468aeb163d8b4585.html. Último acceso: 8 diciembre 2016.

Sagiroglu, S., & Sinanc, D. (2013, May). Big data: A review. In Collaboration Technologies and Systems (CTS), 2013 International Conference on (pp. 42-47). IEEE.

Salom, A., Figueras, J., Ortiz, H., Ortiz, A. I. I. H., Calderón, V., Calderón, M. V., ... & CASTANEDA, J. E. E. C. (2002). Estudio sobre la Ley orgánica de protección de datos de carácter personal (No. 347.121. 1). Argentina.

Saltor, C. E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina.

Sanjuán, T. F. (2005). Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales. Revista de derecho constitucional europeo, (4), 43-86.

Sánchez Rojo, A. (2016). Educación y derecho a la privacidad en la sociedad del conocimiento.

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & de Gea, J. M. C. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Atención Primaria, 46(4), 214-222.

Sapir, A. (2007). Fragmented power: Europe and the global economy (No. 2013/8068). ULB--Universite Libre de Bruxelles.

Sanz, P. L. (2016). Bioética y explotación de grandes conjuntos de datos. La Explotación de Dates de Salud Retos, oportunidades y límites, 25.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company.

Schoenhagen, P., & Mehta, N. (2016). Big data, smart computer systems, and doctor–patient relationship.

Schulz, F. (1946). History of Roman legal science.

Schwartz, P. M. (2013). The EU-US Privacy Collision: A Turn to Institutions and Procedures.

Scott, J. (2014). Extraterritoriality and territorial extension in EU law. American Journal of Comparative Law, 62(1), 87-125.

Senor, I. C., Alemán, J. L. F., & Toval, A. (2012). Gestión del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura. Gaceta Sanitaria, 26(5), 463-468.

Sethi, N. (2014). The promotion of data sharing in pharmacoepidemiology. European journal of health law, 21(3), 271-296.

Shackelford, S. (2012). Fragile merchandise: A comparative analysis of the privacy rights for public figures. American Business Law Journal, 49(1), 125-208.

Shoniregun, C. A., Dube, K., & Mtenzi, F. (2010). Electronic healthcare information security (Vol. 53). Springer Science & Business Media.

Silva, A. C. (2003). Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de

Derecho Informático, (3).

Simon, B. M., & Sichelman, T. M. (2017). Data-Generating Patents. Northwestern University Law Review, 111.

Simmons, B. A. (2001). The international politics of harmonization: the case of capital market regulation. International Organization, 55(03), 589-620.

Singh, S. K., Mani, N., & Singh, B. (2016). A Framework for Extracting Reliable Information from Unstructured Uncertain Big Data. In Intelligent Decision Technologies 2016 (pp. 175-185). Springer International Publishing.

Sligo, J., Gauld, R., Roberts, V., & Villa, L. (2017). A literature review for large-scale health information system project planning, implementation and evaluation. International Journal of Medical Informatics, 97, 86-97.

Smith, C. R. (2011). Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information. Vt. L. Rev., 36, 931.

Smith, K. P., & Christakis, N. A. (2008). Social networks and health. Annu. Rev. Sociol, 34, 405-429.

Snijders, C., Matzat, U., & Reips, U. D. (2012). "Big Data": big gaps of knowledge in the field of internet science. International Journal of Internet Science, 7(1), 1-5.

Social Protection Committee (2014). Adequate social protection for long-term care needs in an ageing society. Recuperado de http://ec.europa.eu/health/ageing/docs/ev_20140618_co04_en.pdf. Último acceso: 6 diciembre 2016.

Solove, D. J. (2013). HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry. Journal of AHIMA, 84(4), 30-31.

Solove, D. J. (2004). The digital person: Technology and privacy in the information age. NyU Press.

Sprenger, M. (2016). E-Health Business Models.

Steinke, G. (2002). Data privacy approaches from US and EU perspectives. Telematics and Informatics, 19(2), 193-200.

Stewart, R., & Davis, K. (2016). 'Big data' in mental health research: current status and emerging possibilities. Social Psychiatry and Psychiatric Epidemiology, 51(8), 1055-1072.

Stylianou, A., & Talias, M. A. (2016). Big data in healthcare: a discussion on the big challenges. Health and Technology, 1-11.

Suárez Conejero, J., Godue, C., García Gutiérrez, J. F., Magaña Valladares, L., Rabionet, S., Concha, J., ... & Liendo Lucano, L. (2013). Competencias esenciales en salud pública: un marco regional para las Américas.

Suciu, G., Vulpe, A., Craciunescu, R., Butca, C., & Suciu, V. (2015, May). Big data fusion for eHealth and Ambient Assisted Living Cloud Applications. In Communications and Networking (BlackSeaCom), 2015 IEEE International Black Sea Conference on (pp. 102-106). IEEE.

Sugiyama, M. S. (2016). Accessing Reliable Health Information On The Internet.

Sunkel, G., & Trucco, D. (2010). Nuevas tecnologías de la información y la comunicación para la educación en América Latina: riesgos y oportunidades. CEPAL.

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association, amiajnl-2013.

Suzman, R., Beard, J. R., Boerma, T., & Chatterji, S. (2015). Health in an ageing world—what do we know?. The Lancet, 385(9967), 484-486.

Tascón, M. (2013). Introducción: Big Data. Pasado, presente y futuro. Telos: Cuadernos de comunicación e innovación, (95), 47-50.

Téllez, F. A. (2005). Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica. In Protección de datos de carácter personal en Iberoamérica: (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003) (pp. 69-84). Tirant lo Blanch.

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, 64, 63.

Tene, O. (2007). What google knows: Privacy and internet search engines. Utah Law Review, Forthcoming.

Terry, N. P., & Francis, L. P. (2007). Ensuring the privacy and confidentiality of electronic health records. U. Ill. L. Rev., 681-735.

Terstegge, J. (2017). The UE´s privacy by default 2.0. Recuperado de https://iapp.org/news/a/the-eus-privacy-by-default-2-0/. Último acceso 19 noviembre 2017.

The 3rd Generation Partnership Project (3GPP). Recuperdo de http://www.3gpp.org/about-3gpp. Último acceso el 17 de diciembre de 2016.

The present and future of data protection in China. Recuperado de http://www.eurobiz.com.cn/present-future-data-protection-china/. Último acceso 1 enero de 2017.

Thomas, K., Grier, C., & Nicol, D. M. (2010, July). unfriendly: Multi-party privacy risks in social networks. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 236-252). Springer Berlin Heidelberg.

Topol, E. (2015). The patient will see you now: the future of medicine is in your hands. Basic Books.

Torres, A. C. (2016). El marco europeo del derecho a la asistencia sanitaria: de los reglamentos de coordinación a la asistencia sanitaria transfronteriza. Revista General de Derecho del Trabajo y de la Seguridad Social, (42), 13.

Ull, G. (2015). Control y privacidad en el ciberespacio. Uso de las cookies por parte de los principales medios digitales españoles.

UNESCO (2005). La Declaración Universal sobre Bioética y Derechos Humanos adoptada por la Conferencia General de la UNESCO. Recuperado de http://portal.unesco.org/es/ev.php-URL_ID=30274&URL_DO=DO_TOPIC&URL_SECTION=201.html. Último acceso: 9 diciembre de 2016.

Vázquez, M. L., Vargas, I., Unger, J. P., Mogollón, A., Silva, M. R. F. D., & Paepe, P. D. (2009). Integrated health care networks in Latin America: toward a conceptual framework for analysis. Revista panamericana de salud pública, 26(4), 360-367.

Van de Kaa, G., & Greeven, M. J. (2016). Mobile telecommunication standardization in Japan, China, the United States, and Europe: a comparison of regulatory and industrial regimes. Telecommunication Systems, 1-12.

Van der Vaart, R., Drossaert, C. H., de Heus, M., Taal, E., & van de Laar, M. A. (2013). Measuring actual eHealth literacy among patients with rheumatic diseases: a qualitative analysis of problems encountered using Health 1.0 and Health 2.0 applications. Journal of medical Internet research, 15(2), e27.

Van Doosselaere, C., Herveg, J., & Silber, D. (2008). Legally eHealth: putting eHealth in its European legal context. European Commission, 00-55.

Van Limburg, M., van Gemert-Pijnen, J. E., Nijland, N., Ossebaard, H. C., Hendrix, R. M., & Seydel, E. R. (2011). Why business modeling is crucial in the development of eHealth technologies. Journal of medical Internet research, 13(4), e124.

Van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., ... & Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. BMC Public Health, 14(1), 1144.

Van Ommen, G. J. B., Törnwall, O., Bréchot, C., Dagher, G., Galli, J., Hveem, K., ... & Solesvik, O. V. (2015). BBMRI-ERIC as a resource for pharmaceutical and life science industries: the development of biobank-based Expert Centres. European Journal of Human Genetics, 23(7), 893-900.

Van Rooij, T., & Marsh, S. (2016). eHealth: past and future perspectives. Personalized Medicine, 13(1), 57-70.

Van Staa, T. P., Goldacre, B., Buchan, I., & Smeeth, L. (2016). Big health data: the need to earn public trust. BMJ: British Medical Journal (Online), 354.

Vásquez Rocca, A. (2015). Byung-Chul Han: La Sociedad de la Transparencia, Cansancio elocuente y Psicopolítica: De lo viral-inmunológico a lo neuronal-estresante. Revista Observaciones Filosóficas 21. Sección Filosofía Contemporánea.

Viceconti, M., Hunter, P., & Hose, R. (2015). Big data, big knowledge: big data for personalized healthcare. IEEE journal of biomedical and health informatics, 19(4), 1209-1215.

Villanueva, F. L. (2011). Salud e internet: más allá de la calidad de la información. Revista española de cardiología, 64(10), 849-850.

Vithiatharan, R. N. (2014). The potentials and challenges of big data in public health.

Vogel, D. (2012). The politics of precaution: regulating health, safety, and environmental risks in Europe and the United States. Princeton University Press.

Voss, W. G. (2014). Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. Journal of Internet Law, 17(9).

Wang, Y., Kung, L., Ting, C., & Byrd, T. A. (2015, January). Beyond a technical perspective: understanding big data capabilities in health care. In System Sciences (HICSS), 2015 48th Hawaii International Conference on (pp. 3044-3053). IEEE.

Wass, S., & Vimarlund, V. (2016, June). Business models in public eHealth. In 24th European Conference on Information Systems, ECIS 2016, 12 June 2016 through 15 June 2016, Istanbul, Turkey.

Watts, D. J. (2004). Six degrees: The science of a connected age. WW Norton & Company.

Web Médica Acreditada. Recuperado de http://wma.comb.es/es/home.php. Último acceso 5 de enero 2017.

Weiss, M. A., & Archick, K. (2016). US-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service.

Wilder-James (2014). Defining Big Data. Forbes Data Driven.

Wildman, J., McMeekin, P., Grieve, E., & Briggs, A. (2016). Economic evaluation of integrated new technologies for health and social care: Suggestions for policy makers, users and evaluators. Social Science & Medicine, 169, 141-148.

Williams, R. (2016). Why is it difficult to achieve e-health systems at scale?. Information, Communication & Society, 19(4), 540-550.

Williams, R. (2010). CDC's Thomas Frieden—protecting health and reducing costs. The Lancet, 376(9754), 1731.

Withington, P. (2016). Utopia, health, and happiness. The Lancet, 387(10033), 2084-2085.

Yavich, N., & Báscolo, E. P. (2016). Current primary health care practices and research challenges in Latin America.

Ye, H., Cheng, X., Yuan, M., Xu, L., Gao, J., & Cheng, C. (2016, November). A survey of security and privacy in big data. In Communications and Information Technologies (ISCIT), 2016 16th International Symposium on (pp. 268-272). IEEE.

Yener, D. (2016). Geographic Information Systems and Its Applications in Marketing Literature. Handbook of Research on Geographic Information Systems Applications and Advancements, 158.

Young, A. R. (2015). The European Union as a global regulator? Context and comparison. Journal of European Public Policy, 22(9), 1233-1252.

Yue, T., Ali, S., Zhang, M., & Pradhan, D. (2016). Standardization Bodies and Standards Relevant for Uncertainty Modelling. Simula Research Laboratory, Technical Report, 5, 2016.

Zalnieriute, M. (2015). An international constitutional moment for data privacy in the times of mass-surveillance. International Journal of Law and Information Technology, 23(2), 99-133.

Zalon, M. L. (2016). Technology and Continuously Learning Health Systems. The Journal of Continuing Education in Nursing, 47(6), 243-245.

Zárraga, E. C. (2015). El mercado único digital. Unión Europea Aranzadi, (10), 103-105.

Zikopoulos, P., & Eaton, C. (2011). Understanding big data: Analytics for enterprise class hadoop and streaming data. McGraw-Hill Osborne Media.

Zhang, Z. (2015). Data management by using R: big data clinical research series. Annals of translational medicine, 3(20).

Zhang, Z. (2014). Big data and clinical research: focusing on the area of critical care medicine in mainland China. Quantitative imaging in medicine and surgery, 4(5), 426-429.

Zheng, Y. L., Ding, X. R., Poon, C. C. Y., Lo, B. P. L., Zhang, H., Zhou, X. L., ... & Zhang, Y. T. (2014). Unobtrusive sensing and wearable devices for health informatics. IEEE Transactions on Biomedical Engineering, 61(5), 1538-1554.

Ziegele, M., & Quiring, O. (2011). Privacy in social network sites. In Privacy Online (pp. 175-189). Springer Berlin Heidelberg.

Recursos legislativos.

Directiva 2016/1148 del Parlamento y del Consejo Europeo, del 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Reglamento 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.

Real Decreto Ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas.

Decreto 38/2012, de 13 de marzo, sobre Historia Clínica y Derechos y Obligaciones de Pacientes y Profesionales de la Salud en Materia de Documentación Clínica.

Ley 1581/2012, de 17 de octubre, estatutaria de protección de derechos personales, de Colombia. Y el Decreto Reglamentario 1377/2013, de 27 de junio, de Colombia.

Ley 787/2012, de 21 de marzo, de protección de datos personales, de Nicaragüa.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ley 8968/2011, de 7 de julio, de protección de la persona frente al tratamiento de sus datos personales, de Costa Rica.

Ley 29733/2011, de 3 de julio, de protección de datos, de Perú. Y su Reglamento, de 13 marzo de 2013.

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.

Ley 2/2011, de 4 de marzo, de Economía Sostenible. Modificación de la LOPD. Disposición final quincuagésima sexta.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010, de Méjico. Y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los

Particulares, de 21 de diciembre de 2011, de Méjico.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (DA. 4a).

Ley 18.331, de 11 de agosto de 2008, de protección de datos, de Uruguay.

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.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196. (Italia)

Bundesdatenschutzgesetz vom 14. Januar 2003 (Alemania).

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.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Ley 25.326, de 2 de noviembre de 2000, de protección de datos personales, de Argentina.

Wet Bescherming Persoonsgegevens de 6 de julio de 2000 (Holanda).

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La Ley 19.628, de 28 de agosto de 1999, sobre la protección de la vida privada, de Chile.

Data Protection Act, de 16 de julio de 1998 (Reino Unido).

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.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Ley 14/1986, de 25 de abril, General de Sanidad.

Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de la Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Constitución Española, de 29 de diciembre de 1978.

Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Loi 2004-801 du 6 août 2004 (Francia).

Privacy Act, 1974 (EE.UU).

ANEXO I

VENICE
15th IMTC 2016
January 21st-23rd

CERTIFICATE OF PRESENTATION

I hereby certify that Professor

.....Alejandro Kress Serilla.....

presented his/her paper at the

15th International Marketing Trends Conference

in Venice on January 21st-23rd 2016

Jean Claude Andreani

Professor Jean-Claude ANDREANI
ESCP Europe
Co-President of the Congress Scientific Committee

International Marketing Trends Conference
Venice-Paris Marketing - c/o ESCP Europe - 79, av de la République - 75543 Paris Cedex 11 - France
Tel : +33 1 45 03 05 35 - Fax : +33 1 42 30 56 90
www.marketing-trends-congress.com

ANEXO II

EMAC, 6 October 2016

Certificate of Participation & Presentation

This is to attest that **Prof. Alejandro Kress,** Universitat Politècnica de Catalunya, Spain, participated in the **7th EMAC Regional Conference**, September 14-16, 2016, Sarajevo, Bosnia and Herzegovina and presented the paper entitled **" PROTECTING DAVID FROM GOLIATH IN THE BATTLE FOR BIG DATA IN EHEALTH".**

Yours Sincerely,

European Marketing Academy
31 Place de Brouckère
1000 Bruxelles

Anne-Laure Marteaux
EMAC Executive Secretary

PLACE DE BROUCKÈRE-PLEIN 31, 1000 BRUSSELS, BELGIUM
Tel: +32-2-226.66.60 - Fax: +32-2-512.19.29
Website http://www.emac-online.org

"Estoy convencido que la mitad de lo que separa a los emprendedores exitosos de los que han fracasado es la perseverancia".

Steve Jobs (1955-2011)

Dr. Federico Kress Hohmann

Dra. Marina Kress Voltz

L. Alejandro Kress Sevilla