

El gran hermano digital monitoriza nuestros datos de salud

BIB\2015\16286

Josep M^a Monguet

Doctor Ingeniero Industrial. Profesor de la UPC. Universitat Politècnica de Catalunya

Enrique Navarro

. Doctor en Derecho. Profesor Titular de Derecho internacional privado. Universidad Rey Juan Carlos Abogado. Socio de Clyde & Co

Alejandro Kress

Licenciado en Derecho ICADE. Abogado

Fernando Moreno Reyes

Doctor en Marketing. Universidad Complutense

Publicación: Revista Aranzadi Unión Europea, N° 10, Sección Doctrina, Octubre 2015

Editorial: Aranzadi

Introducción

Hoy estamos entrando en la era del Big Data, donde las tecnologías de la información en manos de empresas y gobiernos permiten recoger miles de datos personales con multitud de fines; así nos enfrentamos a denuncias como las de el excontratista de la CIA, Edward Snowden, 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 «Owning the Net». Ya en 1949 George Orwell publicó su novela «1984», donde imaginaba 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.

El carácter emergente de este tema a nivel de salud pública y la trascendencia de esta peligrosa evolución deben hacernos reflexionar muy seriamente: ¿quiere esto decir que los individuos hemos perdido el control sobre sus datos personales? ¿está en riesgo la libertad individual en beneficio de grandes compañías y poderosos gobiernos con ilimitados recursos? ¿cómo afectará esta revolución de datos al sector de la salud en los próximos años? ¿mantendremos como ciudadanos algún control sobre sus datos personales más sensibles?

Antecedentes

La primera legislación de protección de datos a nivel mundial fue aprobada en Alemania en el estado de Hesse en 1970; representó el germen de la primera normativa a nivel nacional que entró en vigor en 1979, un hito histórico. Ya en el seno de la UE, se creó un Grupo de Trabajo de Autoridades de Protección de Datos (de acuerdo con el artículo 29 de la norma en vigor, [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) que estudia aspectos como los datos genéticos.

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.

20 años después de la Directiva se ha hecho necesario unificar la HCE 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 HCE, 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-Henarejos A 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.

Objetivos y método

En el entorno actual del Big Data el objetivo de este estudio es constatar una tendencia (liderada por los propios ciudadanos) hacia la homogeneización en Europa de los parámetros a los que se debe adecuar la sanidad digital en relación con la protección de datos, a pesar de que cada Estado miembro de la UE ha implementado la Directiva de 1995 de forma diferente. El conocimiento y aplicación de los parámetros no estarán limitados al sector legal, sino a médicos, ingenieros, profesionales sanitarios y demás actores implicados. Al mismo tiempo, los esfuerzos por encontrar convergencias deben superar diferencias culturales; Delgado LR (2014).

Se puede concluir que debería producirse una convergencia de las políticas de protección de datos en la UE, y son los propios ciudadanos quienes reclaman los mismos derechos y protecciones a nivel europeo. Y además confían más en las instituciones comunitarias que nacionales para liderar este proceso; la nueva regulación vía Reglamento debería eliminar las divergencias y costes asociados para las empresas, pudiendo convertirse en un modelo líder a nivel global.

Para confirmar esta tendencia se han precisado tres fases; se ha analizado (en la primera fase) la literatura científica, (en la segunda fase) se han estudiado las actitudes sobre protección de datos e identidad electrónica en cada país de la Unión Europea de los 27. Y por último (tercera fase) se ha comparado la cultura sobre datos personales en los 27 países. Quedan al descubierto en este análisis las dificultades a las que se enfrenta esta convergencia a nivel paneuropeo, especialmente las diferencias culturales entre Estados miembros. La primera fase ha permitido detectar el todavía limitado interés que esta materia ha despertado en la literatura científica, mientras que la segunda fase revela cómo de dispares son las actitudes de los europeos hacia la protección de datos. Finalmente la comparativa de la cultura de protección de datos 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 personales (según datos procedentes del Eurobarómetro especial 359 de la Comisión Europea sobre «actitudes sobre protección de datos e identidad electrónica en la Unión Europea», publicado en Junio de 2011). Los datos que revelan las fases de este método desarrollado permiten detectar dónde debe prestarse mayor atención para lograr una eficiente convergencia. 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.

I. Big Data en eHealth y privacidad

En este apartado se abarca el concepto de Big Data, en el contexto de la salud digital, desde la perspectiva de la privacidad. Todavía se tiene un conocimiento muy limitado sobre el Big Data (Snijders C et al, 2012) que ha llegado al ámbito de la salud, donde confluyen multitud de datos provenientes de numerosas y variadas fuentes. La UE trabaja en un nuevo marco regulatorio de protección de datos 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 la salud digital, aunque algunos investigadores médicos reconocen que proteger la privacidad de los datos del paciente resulta casi imposible (Enserink y Chin, 2015).

Una parte muy significativa de lo que hoy se llama Big Data es información sobre nosotros mismos, así lo creen Terence C y Ludloff M (2011), quienes estiman 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. El Presidente y co-fundador (en 1982) de Sun Microsystems, Scott McNealy, dijo en 1999 que debemos resignarnos al hecho de no tener privacidad: «You already have zero privacy. Get over it»; Solove D (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 C y Raab C (2006). Algunos creen que sólo con ejemplos de la vida real se puede justificar la necesidad de compartir datos para mejorar la atención sanitaria (Heitmueller A et al, 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); 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 personales, 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; Arenas M (2006).

Así todo, Terence C y Ludloff M creen que los datos personales son el activo más valioso hoy en día, «más que el oro. Los individuos somos el activo que toda compañía, industria, ONG o gobierno desea». 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, 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 suplente 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.

La gestión de la HCE implica unos desafíos técnicos y legales. Los posibles beneficios que ofrecen los sistemas de Historia Clínica Electrónica (HCE) 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 personales 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.

Garrie DB y Wong R (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 de protección de datos 95/46/CE ; y la Directiva sobre la privacidad y comunicaciones electrónicas 2002/58/CE) y el marco jurídico de los Estados Unidos, 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 personales 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 MC (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, no existe una clara definición del concepto de datos encriptados. En este artículo el autor 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. Sin este marco la investigación médica transnacional nunca será realmente efectiva ⁽¹⁾.

Derecho a la privacidad en la UE versus EE.UU.

La literatura científica trata de evaluar si 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 humano básico que debe ser protegido a toda costa (Steinke G, 2002; Shackelford, S, 2012; Voss WG, 2014); mientras que la UE considera la intimidad como un derecho inalienable, los EE.UU parecen tratar los datos personales más como una mercancía o un bien. En China el derecho a la privacidad, o más bien su ausencia, representa hoy el extremo opuesto al de la UE.

En EE.UU no existe una única norma referida a la privacidad electrónica ⁽²⁾; la HIPAA ⁽³⁾ cubre el sector sanitario. Los derechos del individuo son contemplados más bien como «consumer rights» en 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 ⁽⁴⁾, 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 debe recibir 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. Sin embargo, es cierto que su modelo se basa en considerar la privacidad como un bien o mercancía, dejando en manos del consumidor su protección y posibles demandas hacia una mayor regulación.

Uso de los datos personales.

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, al margen del juramento hipocrático y de la debida confidencialidad entre médico y paciente, puesto que dichos principios, en el contexto tecnológico actual, han perdido su operatividad y eficacia.

La posibilidad de que las empresas puedan obtener datos sin el consentimiento del interesado sigue levantado mucha controversia en Europa, y siendo motivo de algunas resoluciones de los organismos reguladores. En concreto, 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». El concepto de individuo con sus derechos fundamentales en Europa se distingue así del de lo que en EE.UU se considera simplemente un consumidor.

El modelo europeo se impone como líder en la defensa de una estricta protección de la privacidad a favor de los individuos ⁽⁵⁾.

La [Convención Europea de Derechos Humanos](#) ⁽⁶⁾ 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. Hoy la evolución del modelo europeo acentúa las divergencias con el norteamericano; Martínez R (2014).

Varias Constituciones Europeas, como la alemana, recogen el derecho a la privacidad ⁽⁷⁾. Antes de 1995 existían en Europa distintas leyes sobre privacidad; así el órgano de control del cumplimiento de la normativa de protección de datos en España es la Agencia Española de Protección de Datos (AEPD) creada en 1994 ⁽⁸⁾.

En 1995 se hizo por primera vez referencia a la protección de la personal físicas en lo que respecta al tratamiento de datos personales 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 ⁽⁹⁾.

De esta forma se desarrolla una normativa adaptada a la Directiva en cada Estado miembro y en España la norma española fundamental de referencia en esta materia ⁽¹⁰⁾ se refiere expresamente a los datos de salud, (considerándolos especialmente protegidos y limitando la posibilidad de su recopilación y cesión), aunque no define su concepto. Esta ley 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.

Por otro lado, el Comité de Ministros del Consejo de Europa en su Recomendación n°5, de 13 de febrero de 1997, referida a la protección de datos médicos, establece 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 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 ⁽¹¹⁾.

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 ⁽¹²⁾. En EE.UU el gasto en salud representó en 2012 el 17.2% del PIB ⁽¹³⁾, 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 y 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 C, Whitehouse D, Duquenoy P (2013). Estos autores 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 DW (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 manejar 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.

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 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 bienestar, más allá del potencial, todavía queda lograr una efectiva mejora de la salud junto con una reducción de costes; Williams R (2010).

El plan de acción de la UE ⁽¹⁴⁾ pretende incrementar el ritmo de cambio y mejora de la atención sanitaria mediante las siguientes medidas:

aclarando áreas de inseguridad jurídica;

mejorando interoperabilidad entre sistemas;

aumentando la concienciación 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 ⁽¹⁵⁾. 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 ⁽¹⁶⁾. De hecho, la falta de mayores mecanismos de control gubernamental ha supuesto hasta ahora una barrera para obtener la confianza de los ciudadanos/pacientes para el desarrollo del HCE; Terry N y Francis L (2007).

Ya en 2008 se emitió la primera Recomendación sobre HCE interoperativos. Para que estos HCE sean interoperativos 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 BM (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.

II. Las actitudes de los ciudadanos europeos

En este apartado se trata sobre las diferentes actitudes de los europeos, en función de su país de origen, respecto a la privacidad, y se pretende con ello constatar la tendencia a la armonización liderada por los propios europeos. Una gran mayoría de los europeos entrevistados ⁽¹⁷⁾ (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 1), 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.

Tabla 1
Actitudes de la 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%). 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 (figura 1).

Figura 1

Confianza de los ciudadanos europeos en sus Instituciones

Imagen

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 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 2); 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.

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 puedan estar a disposición de compañías públicas o privadas.

Tabla 2.

Valoración de la datos personales por sexo, edad, estudios, profesión, uso de Internet, capacidad adquisitiva y escala social.

	Consideran la información médica como dato personal	Consideran 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 Internet ⁽¹⁸⁾ (tabla 3); 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.

Autorización paterna 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 suscripción 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 personales 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 personales puede ayudar a una mayor concienciación sobre su trascendencia, a la vez que puede animarles a ser más prudentes a la hora de revelar datos personales. 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%).

III. La adaptación a un marco legal unificado

En este tercer apartado se señalan los desafíos, incluidos los entornos culturales, para el desarrollo de sistemas integrados de eHealth a nivel internacional. Como señalan Bates DW y Wright A (2009), a pesar de las numerosas oportunidades que existen para la colaboración internacional, 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. A pesar de los avances recientes en materia de traducción automática, el 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. 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 los proveedores de servicios sanitarios, y especialmente entre los propios pacientes. Pero según estos autores, 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 et al (2005) estas diferencias incrementaron en 150 días en el estudio de una multinacional, y de

acuerdo con la investigación de Hearnshaw H (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 WG et al. (2014). La UE se 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, parece que 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»⁽¹⁹⁾; 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⁽²⁰⁾; 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.

El camino hacia la armonización

No son pocos los retos, la Europa de los 27 ha implementado la normativa de 1995 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 completa está en camino, a través de la jurisprudencia⁽²¹⁾ y del nuevo Reglamento; esta nueva legislación que se debe aprobar en el Parlamento Europeo para la armonización puede poner serias trabas a la investigación epidemiológica y médica en general (Ploem MC et al, 2013).

El artículo 7 f) de la Directiva⁽²²⁾ establece que los Estados miembros dispondrán que el tratamiento de datos 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»⁽²³⁾.

Por otro lado, el TJUE⁽²⁴⁾ define el alcance normativo de la norma señalando que no admite que las normativas nacionales, en ausencia del consentimiento del interesado, exijan para permitir el tratamiento de datos personales «necesario para la satisfacción de un interés legítimo», 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 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 personales sin el consentimiento del afectado^{(25) (26)}.

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](#), «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 están de acuerdo en que este tipo de iniciativas supongan una mejora efectiva⁽²⁷⁾.

La interoperabilidad.

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. Y el mismo 2011 se lanza epSOS («Smart Open Services for European Patients»), el proyecto europeo de eHealth que incluye 23 países, donde España es líder con dos autonomías que engloban más pilotajes que el resto de países participantes juntos.

Así, la Agenda Digital para Europa incluye proyectos y acciones específicas de eHealth. A pesar de la crisis económica actual 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, 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.

La gestión de la información sanitaria.

Para Kankanady R y Well M (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 autenticación, 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 A et al, 2014).

En cuanto a las políticas de acceso a los sistemas de HCE, 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» (Carrión i et al, 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 U (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⁽²⁸⁾.

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 M et al (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.

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 personales 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 B (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 ⁽²⁹⁾. 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 ⁽³⁰⁾. Respecto a los EE.UU (sin perjuicio de que sigue siendo un país que no ofrece, según la normativa comunitaria, un nivel de protección equiparable o adecuado), se reconoce el nivel adecuado a las entidades estadounidenses adheridas a los principios de «Puerto Seguro». Canadá solamente respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, y los datos personales 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, y sólo lo harán a países que adopten el modelo europeo. Así, distintos países latinoamericanos parecen empezar a implantar el modelo europeo de protección de datos; algunos por motivaciones meramente económicas (para poder acoger centros de datos que pueden convertirse en la fuente de un negocio muy lucrativo). Todo esto 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 unificada de privacidad internacional.

Resultados y conclusiones

¿Qué añade este artículo a la literatura? En conclusión se quiere contribuir a valorar la magnitud de los avances en materia de eHealth y protección de datos en la UE, y deja a la vista cuál será la tendencia en los próximos años. La normativa de la UE está avanzando hacia el doble objetivo de una eficiente implementación de la HCE y la efectiva protección de la privacidad, donde el ciudadano debe ejercer el control. Por ello la concienciación desempeña un papel central pues sin ella los individuos no podrán ejercer sus derechos incluso ante los tribunales. 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. 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 ⁽³¹⁾. 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.

En el futuro será preciso extremar la ponderación de las circunstancias que concurran en cada supuesto concreto para decidir sobre la legitimidad del tratamiento. 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 ⁽³²⁾; el futuro Reglamento europeo de protección de datos ⁽³³⁾ 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 sustituir la actual normativa, 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). 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.

La armonización integral no será fácil en la UE pero si se produce traerá 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 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 del ciudadano europeo, frente a países como EE.UU donde la libertad del individuo parece quedar supeditada a intereses mercantilistas. La UE se ha posicionado a favor del avance tecnológico pero no a costa de los derechos fundamentales del ciudadano.

Al mismo tiempo, el concepto de privacidad está evolucionando, y nos debería hacer reflexionar si el Big Data no lleva dentro de su ADN la posibilidad de contribuir al control de quien 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. Este artículo es por ello sólo una reflexión en el camino, nunca un punto y final.

Referencias:

- Arenas M (2006): «El Derecho Fundamental a la Protección de Datos personales en Europa», Tirant Lo Blanch.
- Bates DW (1997): «Commentary: Quality, Costs, Privacy and Electronic Medical Data», Journal of Law, Medicine and Ethics, vol. 25, issues 2 & 3, pp. 111-112.
- Bates DW, Wright A (2009): «Evaluating eHealth: Undertaking Robust International Cross-Cultural eHealth Research», PLoS Med 6(9): e1000105. doi:10.1371/journal.pmed.1000105.
- Bennett C, Raab C (2006): «The Governance of Privacy». Policy Instruments in Global Perspective, The MIT Press, Cambridge-Londres, pp. 8 y 298.
- Carrión I et al (2012): «Gestión del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura», Gaceta Sanitaria, v26 n5, pp. 463-468.
- Comisión Europea, Eurobarómetro especial 359 (2011): «Actitudes sobre protección de datos e identidad electrónica en la Unión Europea».
- Comisión Europea, MEMO/12/959 del 7 de diciembre de 2012.
- Comisión Europea, MEMO/13/1059 del 27 de noviembre de 2013.
- Delgado LR (2014): «Vida privada y protección de datos en la Unión Europea». Midac.
- Elwyn G, Seagrove A, Thorne K, Cheung WY (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, vol. 347, no. 6221, pp. 490-491.
- European Commission Information Society and Media Directorate-General (2011): «Report on the public consultation on eHealth Action Plan 2012-2020».
- Franzkiska B (2011): «Information Sharing and Data Protection in the Area of Freedom, Security and Justice», Springer.
- George C, Whitehouse D, Duquenoy P (2013): «eHealth: Legal, Ethical and Governance Challenges», Springer.
- Garrie DB, Wong R: «The Future of Consumer Web Data: A European/US Perspective», International Journal of Law and Information Technology, vol. 15, issue 2 (2007), pp. 129-152.
- Hearnshaw H (2004): «Comparison of requirements of research ethics committees in 11 European countries for a non-invasive interventional study», BMJ 328: 140-141.
- Heitmüller A et al (2014): «Developing Public Policy To Advance The Use Of Big Data In Health Care», Health Affairs, vol. 33, no. 9, pp. 1523-1530.
- Herveg J et al (2008): «The protection of medical data: Challenges of the 21st century», 79-88.
- Hiller J et al (2011): «Privacy and Security in the Implementation of Health Information Technology» (Electronic Health Records).
- Herveg J (2014), «Data Protection and the Patient's Right to Safety», European Journal of Health Law, vol. 21, issue 3, pp. 260-270.
- Kankanady R, Wells M (2013): «Health Information Governance in a Digital Environment», E.J.S. Hovenga and H. Grain, pp. 209-230.
- Knoppers BM (2005): «Biobanking, international norms», The Journal of Law, Medicine & Ethics, vol. 33, issue 1, pp. 7-14.

- Martin AB et al (2014): «National health spending in 2012: rate of health spending growth remained low for the fourth consecutive year», Health Affairs, vol. 33, no 1, pp. 67-77.
- Martínez R (2014): «Privacidad, Estados Unidos y España. Tan lejos, tan cerca.» Telos (Cuadernos de Comunicación e Innovación), pp. 48-56.
- Osborne Clarke (2012), informe: «La fiebre del oro de los datos».
- Ploem MC (2006): «Towards an Appropriate Privacy Regime for Medical Data Research», European Journal of Health Law, vol. 13, issue 1, pp. 41-64.
- Ploem MC et al (2013): «Proposed EU data protection regulation is a threat to medical research», BMJ, vol. 346.
- Rauer U (2012): «Patient Trust in Internet-based Health Records: An Analysis Across Operator Types and Levels of Patient Involvement in Germany, Policy & Internet», v4 n2, 1-42. doi: 10.1515/1944-2866.1177.
- Sánchez-Henarejos A et al (2014): «Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria», Atención Primaria, vol. 46, no 4, pp. 214-222.
- Shackelford SJ (2012): «Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures». American Business Law Journal, vol. 49, issue 1, pp. 125-2008.
- Snijders C et al (2012): «Big Data: Big Gaps of Knowledge in the Field of Internet Science», International Journal of Internet Science, vol. 7, issue 1, pp 1-5.5.
- Solove D (2004): «HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry», Journal of AHIMA 84, no.4; pp. 30-31.
- Solove D (2004): «The Digital Person». Technology and Privacy in the Information Age, New York University Press, 2004, pp. 224.
- Steinke G (2002): «Data privacy approaches from US and EU perspectives». Telematics and Informatics, vol. 19, no 2, pp. 193-200.
- Terence C, Ludloff M (2011): «Privacy and Big Data», Sebastopol/O'Reilly Media.
- Terry N, Francis L (2007): «Ensuring the Privacy and Confidentiality of Electronic Health Records», University of Illinois Law Review, vol. 2007, pp. 681-735.
- Van der Vaart R, D Constance, De Heus M, Taal E, Van de Laar M (2011): «Measuring Actual eHealth Literacy Among Patients With Rheumatic Diseases: a Qualitative Analysis of Problems Encountered Using Health 1.0 and Health 2.0 Applications», J Med Internet Res 2013, 15(2): e27.
- Voss WG (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, vol. 17, no 9.
- Van Panhuis, WG et al (2014): «A systematic review of barriers to data sharing in public health», BMC public health, vol. 14, no 1, pp. 1144.
- Williams R (2010): «CDC's Thomas Frieden—protecting health and reducing costs», Lancet, 376.

- (1) El artículo 27 de la Directiva 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».
- (2) Terence C y Ludloff M señalan en su libro «Privacy and Big Data» que existe un modelo de especial regulación centrado especialmente en dos sectores (financiero y sanitario) y en el ámbito de los menores de 13 años.
- (3) Health Insurance Portability and Accountability Act» de 1996.
- (4) Según se recoge en la COPPA («Children's Online Privacy Protection Act»).
- (5) Para Terence C y Ludloff M apuestan así por la teoría del control de los individuos en el modelo europeo.
- (6) 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».
- (7) 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».
- (8) 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.
- (9) [Directiva Europea 95/46 CE](#) de 24 de octubre del Parlamento Europeo y del Consejo.
- (10) [Ley Orgánica 15/1999 de Protección de Datos](#) de Carácter Personal (LOPD).
- (11) 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](#).
- (12) Según datos de la OCDE.
- (13) Martin AB et al (2014): «National health spending in 2012: rate of health spending growth remained low for the fourth consecutive year», Health Affairs, vol. 33, no 1, p. 67-77.
- (14) MEMO/12/959 de la Comisión Europea, del 7 de diciembre de 2012.

- (15) European Environment & Health Action Plan 2004-2010.
- (16) Que sirvió de base para el nuevo «eHealth Action Plan 2012-2020», que a su vez responde a la petición de 2009 de los Estados miembros.
- (17) Datos procedentes del Eurobarómetro especial 359 sobre «actitudes sobre protección de datos e identidad electrónica en la Unión Europea», publicado en Junio de 2011.
- (18) Según un 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.
- (19) Hiller J et al (2011), «Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared».
- (20) Hiller J et al (2011), «Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared».
- (21) 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](#), 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.
- (22) La Sentencia proclama que el artículo 7f) tiene efecto directo.
- (23) 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](#).
- (24) Tribunal de Justicia de la Unión Europea.
- (25) 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.
- (26) 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».
- (27) Herveg J (2014), «Data Protection and the Patient's Right to Safety».
- (28) 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.
- (29) 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».
- (30) Suiza, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Noruega, Islandia, Liechtenstein, Israel y Uruguay y Nueva Zelanda.
- (31) Comisión Europea, Eurobarómetro especial 359 (2011).
- (32) La Comisión Europea propuso en 2012 una reforma para armonizar la forma en se recogen los datos, su acceso y uso, el futuro Reglamento de protección de datos.
- (33) El 12 de marzo de 2014 el Parlamento Europeo dio luz verde al proyecto de Reglamento Europeo de Protección de Datos.