IMPLANTACIÓN DEL CHIP SUBCUTÁNEO: PROTECCIÓN DE DATOS, INTIMIDAD Y LIBERTAD RELIGIOSA

VERÓNICA ALARCÓN SEVILLA

Abogada. Directora Jurídica y de Privacidad de *ePrivacidad*.

Profesora Asociada de Derecho Civil

Universidad de Murcia

v.alarcon@um.es

MARAVILLAS ALICIA CARMONA ABRIL

Abogada. Asesora Jurídica y de Privacidad de *ePrivacidad.*

RESUMEN: Los rumores que planean de una futura implantación obligatoria de chip subcutáneos en humanos con finalidades de identificación, almacenamiento de datos sanitarios o incluso con funciones de geolocalización, es un hecho que desde hace más de una década subyace en la sociedad, y aunque por el momento no se ha mostrado en España una voluntad política de desarrollar una ley específica que contenga su regulación la existencia por el avance tecnológico, de chip aptos para uso humano es ya una realidad, y su incidencia en nuestra vida cotidiana es cada vez mayor: chips implantados en mujeres canadienses afectadas de osteoporosis que libera fármacos a la hora y con la dosis indicada o chips en ciclistas argentinos diabéticos que miden continuamente sus niveles de glucosa; puede traer consigo que la obligatoriedad de su implantación se lleve a cabo por golpe de Ley en cualquier momento. No obstante y aunque aún quedaría mucho camino por recorrer, con este estudio se pretende abordar la problemática que su

uso podría suscitar en materia de derechos fundamentales como la protección de datos en el ámbito sanitario, señalando algunas previsiones para un adecuado marco jurídico futuro, así como su injerencia directa en el derecho a intimidad del ser humano o en el plano de la religiosidad.

PALABRAS CLAVE: Chip subcutáneo, protección de datos, intimidad, libertad religiosa, historia clínica.

SUMARIO: I. Los antecedentes inmediatos. II. Hacia su posible en regulación EE.UU. y Europa. III. Colisión con los derechos fundamentales de protección de datos y libertad religiosa. III.1 Consideraciones y repercusiones jurídicas en la propiedad, custodia, conservación, acceso y rectificación de los datos sanitarios; III.2 ¿Invasión a la intimidad?; III.3 Libertad religiosa versus El número 666 de la bestia.

I. LOS ANTECEDENTES INMEDIATOS

La Real Academia de la Lengua Española, define chip como "pequeño circuito integrado que realiza numerosas funciones en ordenadores y dispositivos electrónicos"; definición que en un corto periodo de tiempo ha quedado obsoleta, ya que la implantación de un chip subcutáneo en individuos ha dejado de ser una utopía para convertirse en una realidad inmediata[1].

[1] Los ejemplos son varios. Es el caso de Robert Nelson, un ciudadano norteamericano que lleva implantado un chip NFC bajo la piel de la mano, para pretender con ello *"abrir la puerta de su casa, la de su coche o la del garaje",* informaba el diario digital ComputerHoy.com. Accesible en http://computerhoy.com/noticias/hardware/hombre-implanta-chip-nfc-su-propia-mano-20035

O el de Kevin Warwick, profesor de cibernética en la Universidad de Reading (Reino Unido) que según eldiario.es *"decidió dejar de ser un limitado mortal en 1998. "Nací humano, pero fue por un accidente del destino, una condición simplemente de tiempo y lugar. Creo que es algo que tenemos el poder de cambiar". El científico se implantó un microchip en el brazo con el que abría las puertas y encendía la luz o la calefacción. En 2002 dio un paso más allá: una interfaz neuronal implantada en su sistema nervioso le permitía controlar un brazo robótico."* Accesible en: http://www.eldiario.es/hojaderouter/tecnologia/hardware/microchip-RFID-cyborg-implantes-NFC_0_301320505.html

Su origen se remonta al año 2001 cuando la corporación estadounidense Applied Digital Solutions, Inc, anunció el desarrollo de un chip miniaturizado de identificación implantable en humanos y denominado VeriChip, que pasó a ser el primer chip apto para humanos al ser aprobado por la Food & Drug Administration de los EE.UU en 2004[2].

El dispositivo, del tamaño aproximado de un grano de arroz, se implanta de forma subcutánea en humanos y contiene informaciones relativas a su portador que le han sido grabadas y que pueden recuperarse por un sistema de identificación por radiofrecuencia (RFID). Su funcionamiento es sencillo, una vez implantado, se escanea usando la frecuencia correcta y el VeriChip responde con un número único de 16 dígitos que puede ser vinculado con información sobre el usuario y almacenada en una base de datos. Este chip sirve tanto para la verificación de identidad, como el acceso a los registros médicos u otros posibles usos que podrían atribuírsele en el futuro.

Frente a ese hipotético escenario de que un chip sea implantado en humanos, ya no de manera voluntaria, sino de forma obligatoria a través de los ordenamientos jurídicos de los países más desarrollados, tanto legisladores como juristas, hemos de plantearnos si dichos dispositivos serían afines a la aparición de instrumentos que actualmente están proliferando en su uso como son los wearables[3], o si por las características del chip y los peligros que podrían entrañar y que analizaremos más adelante, deberían ser regulados de forma minuciosa en leyes específicas al respecto.

---

[2] Este chip, se comercializa por la Corportación VeriChip, perteneciente a Applied Digital Solution, Inc, corporación matriz y creadora de ese nano-chip. Asimismo, de su desarrollo, tecnología, almacenamiento de datos y su recuperación, se está encargando una filial de Applied Digital Solution llamada Destron. Por su parte, U.S Food and Drug Administration – Protecting and Promoting Your Healt, es un organismo estadounidense responsable de: *Proteger la salud pública mediante la regulación de los medicamentos de uso humano y veterinario, vacunas y otros productos biológicos, dispositivos médicos, el abastecimiento de alimentos en nuestro país, los cosméticos, los suplementos dietéticos y los productos que emiten radiaciones*.

[3] También denominados wearable computing o tecnología para llevar puesta según la Nota Informativa *Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre internet de las cosas*, dictamen en el que identifica y alerta *de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades y realizando recomendaciones*. La nota está disponible en https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/sep_14/140924_NP_AEPD_Dictamen_IoT.pdf

Ante dicha cuestión, hay que poner de manifiesto que un chip subcutáneo no es un instrumento afín a un wearable, básicamente por dos razones: la primera de ellas, es que el usuario puede desprenderse de un dispositivo wearable en cualquier momento, a diferencia de lo que ocurre con el chip, que una vez implantado bajo la piel no puede ser sustraído fácilmente; y en segundo lugar, tomando como ejemplo el VeriChip, y a diferencia de un wearable no es un sistema de implantación de posicionamiento por satélite, por el momento VeriChip[4].

Son diversos los problemas que podría plantear la obligatoriedad de la implantación de un chip subcutáneo en humanos y los riesgos inherentes al uso mismo, ya no sólo en materia de fabricación, distribución y utilización, sino su posible colisión con diversos derechos fundamentales, problemas de seguridad con los datos almacenados y otros problemas de índole moral que intentaremos abordar en este estudio, pero ¿somos realmente conscientes de las consecuencias de su uso? ¿Estamos realmente preparados para que los gobiernos obliguen a sus ciudadanos a implantarse un chip subcutáneo?

II. HACIA SU POSIBLE REGULACIÓN EN EE.UU Y EUROPA

La posibilidad de que por Ley sea obligatorio que las personas deban insertarse un chip subcutáneo, es una eventualidad que coadyuva de alguna forma con la evolución de la humanidad y el avance de las nuevas tecnologías hacia un mundo más automatizado. Corolario de la anterior afirmación, es que hemos sido conocedores de diversas informaciones que apuntaban a que a los bebés nacidos a partir de mayo 2014 en los hospitales públicos de Europa les sería implantado un chip subcutáneo[5], o de las noticias referentes a la Ley de reforma de la salud pública, que

[4] Al respecto, *Aspectd Éthiques des implants TIC dans le corps humain,* adoptado el 16 de marzo de 2005, pág.9. Disponible en: http://appel.lsf.free.fr/Docs/GEE_avis20.pdf

[5] Según el medio italiano *Corrieredіroma, la instauración del chip en toda la población europea estaba prevista para el año 2017 y j*unto con el chip, una vez implantado, había que entregar una hoja de datos relativos a la persona portadora (nombre, tipo de sangre, fecha de nacimiento, etc). Este chip también tendría funciones de detector GPS estando conectado directamente a un satélite y que permanentemente tendría localizada al portador del chip. *La información, que finalmente fue desmentida, aún se encuentra disponible en* http://www.corrieredіroma.it/2013/12/microchip-obbligatorio-per-tutti-i-neonati-da-maggio-2014/.

ha pasado a conocerse como ObamaCare[6] y que el actual presidente del gobierno de los Estados Unidos, Barack Obama, ha logrado instaurar en su país.

Los rumores que se extendieron sobre su implantación obligatoria de entrar en vigor la ley, alarmó a medio mundo y ello por una errónea interpretación de sus preceptos.

En efecto, el "chip myth" o "mito del chip", no dejó de ser una especie de bulo legal, tal vez de los más sonados que se recuerden; y es que debemos adelantar que la *Ley Obamacare* no contiene, ni contenía mención alguna acerca de un implante de chip RFID en humanos de forma obligatoria[7]. Su origen parece encontrarse en una versión anterior de la Ley, la H.R.3200 del año 2009 que incluía una sección que permitía que diversos datos fuesen recogidos en dispositivos de clase II entre los que se incluían chips RFID[8].

No obstante, sí encontramos menciones al chip RFID en la sección 519 de la Ley *"Federal Food, drug, and cosmetic act subchapter V – drugs and devices"* de Estados Unidos, existiendo actualmente la posibilidad de injertar un chip subcutáneo, no obligatorio, pero que sí permitiría la recogida de datos del dispositivo implantado[9].

Asimismo y a pesar de los desmentidos, existen informaciones que revelan que la *Food & Drug Administration* ha establecido normas para un sistema de implantación de chip de radio frecuencia en humanos (chip RFID). Estos chip contendrían básicamente información de índole sanitaria, como la identificación del paciente e historia clínica.

---

[6] Denominada Patient Portection and Affordable Care Act – Ley de Protección al Paciente y Cuidado de salud Asequible, fue promulgada con carácter de ley por el presidente de los Estados Unidos Barack Obama el 23 de marzo de 2010. Disponible en: http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf.

[7] Sobre el mito, http://obamacarefacts.com/obamacare-microchip-implant/.

[8] Disponible en: http://www.gpo.gov/fdsys/pkg/BILLS-111hr3200rh/pdf/BILLS-111hr3200rh.pdf. La recogida de los datos de las personas que llevasen implantado este chip iba encaminada a para facilitar el análisis de la seguridad y los resultados de los datos postmarket de los chips RFID implantados.

[9] Disponible en: http://www.gpo.gov/fdsys/pkg/USCODE-2010-title21/html/USCODE-2010-title21-chap9-subchapV-partA-sec360i.htm

En definitiva, si bien la posibilidad del implante de un chip subcutáneo en la *Ley ObamaCare* quedó en un mito, los chips RFID no lo son, y parece ser evidente y en EE.UU son conscientes de ello, que con ese tipo de dispositivos se pueden llegar a conseguir gran cantidad de beneficios en el futuro[10].

III. COLISIÓN CON LOS DERECHOS FUNDAMENTALES DE PROTECCIÓN DE DATOS, INTIMIDAD Y LIBERTAD RELIGIOSA

Directamente relacionado con la implantación del chip subcutáneo en humanos y como premisa a tener en cuenta, la Ley 41/2002 dispuso como principio básico que toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes usuarios[11], estableciendo como forma de su prestación la verbal. Sin embargo, la propia norma señala, como excepciones, los supuestos en los que será necesario el consentimiento escrito de paciente, entre los que se encuentran la intervención quirúrgica y la aplicación de procedimientos que suponen riesgos de notoria y previsible repercusión negativa sobre su salud[12]. Se entiende pues, a falta de ley en contrario, que para poder implantar un chip en el cuerpo humano se precisará el consentimiento libre e inequívoco del interesado por escrito, toda vez que a tal fin se precisa de una intervención quirúrgica y al estar compuestos por silicio parece causar efectos negativos sobre la salud de su portador[13]. Pero su implantación voluntaria o posiblemente obligatoria, puede no ser respetuosa con la intimidad, protección de datos y libertad religiosa, y las previsiones que recogió nuestro legislador son a todos luces insuficientes y obsoletas a fin de respetar esos derechos, siendo necesaria una regulación específica que atienda a las peculiaridades que se deriven de la implantación del chip en el cuerpo humano.

[10] Para ampliar información http://obamacarefacts.com/obamacare-microchip-implant/

[11] Artículo 2.2.

[12] Artículo. 8.2

[13] Sobre sus efectos, ALBRECHT, K., en Synopsis of "Microchip Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006", proporciona una revisión detallada de literatura publicada en revistas de toxicología y patología que muestran una relación de causalidad entre el chip y cáncer en roedores de laboratorio y perros y que han llevado a una preocupación generalizada sobre la seguridad de los chips implantables en animales y seres humanos. Disponible en: http://www.antichips.com/cancer/albrecht-microchip-cancer-synopsis.pdf

III.1 Consideraciones y repercusiones jurídicas en la propiedad, custodia, conservación, acceso y rectificación de los datos sanitarios

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 historia clínica en su artículo 3 como *"el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial";* definición que hay que completarla con otra más descriptiva contenida en el artículo 14 bajo la rúbrica "*Definición y archivo de la historia clínica*", según el cual comprende el "*conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro*". Pero además de su extraordinario valor médico en el proceso asistencial, y jurídico en los casos de responsabilidad profesional, constituye un fichero de datos de carácter personal[14] y por tanto le será de aplicación no sólo las prescripciones de la Ley 41/2002 si no también las reglas generales del tratamiento de datos que sin atender a especificidades en el ámbito sanitario están contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Sin embargo, la evolución -de la mano del avance tecnológico- del formato de almacenamiento, recuperación y visualización de los documentos que integran la historia clínica -del soporte en papel tradicional al electrónico y a su implementación en el cuerpo humano-, llevará aparejado la discusión y debate de muchos aspectos legales relacionados con la titularidad, acceso, y custodia y conservación de la información contenida en el chip subcutáneo.

[14] La Ley 15/1999 define en su artículo 3 como fichero "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*" y ese carácter de fichero de la historia clínica ha sido admitido por la Agencia Española de Protección de Datos en distintos informes de su Gabinete Jurídico, por ejemplo, informe número 0551/2008, en remisión todos ellos a uno anterior de fecha 12 de noviembre de 2007 no publicado, al señalar "*Por este motivo, el profesional se encontrará obligado al cumplimiento de las obligaciones legalmente previstas en relación con su fichero de historias clínicas (...)*".

La propiedad de la historia clínica ya suscitó muchas discusiones doctrinales que se plasmaron en distintas teorías, una que defiende que es propiedad del paciente partiendo de la consideración que los datos que en la historia se incluyen les atañe, otra que mantiene que le pertenece al médico por ser una creación intelectual y científica suya, y otra que sostiene que es de la institución sanitaria como garante de su conservación, sin faltar las teorías eclécticas o integradoras de las tres anteriormente expuestas[15].

Parece claro que, la barrera financiera para la implantación del chip en pacientes por la administración sanitaria debido a los altos costes asociados a una inversión inicial y a su posterior mantenimiento, así como a la falta de infraestructura informática adecuada y fuentes de financiación, añadirán una nueva teoría al listado, la que se fundamenta en el hecho de que su propiedad correspondería a la empresa de base tecnológica que decidiese aportar sin coste el soporte y lo mantuviese. En efecto, en los últimos años grandes compañías multinacionales con sede en Estados Unidos Y especializadas en software, dispositivos electrónicos y tecnologías en general, están ofreciendo servicios aparentemente gratuitos. Son el caso del servicio HealthVault de Microsoft[16] o Google Health de Google Inc, servicio este último que hasta el 1 de enero de 2012 permitió a sus usuarios registrar voluntariamente información de salud como resultados de exámenes, medicamentos, datos del seguro, alergias, etc. y acceder a ella a través de internet. Junto a Google, participaron en el proyecto empresas farmacéuticas y de investigación[17]. La misma teoría ha de predicarse respecto de aquellas personas que voluntariamente ya llevan estos circuitos integrados en su cuerpo.

Lo anterior hay que conectarlo necesariamente con las previsiones establecidas en la Ley básica a efectos de su custodia y conservación. Si en principio

[15] Sobre la titularidad, CODÓN HERRERA, A., «La historia clínica: concepto, normativa, titularidad y jurisprudencia » en *Autonomía del paciente, información e historia clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, 2004, págs. 146-156.

[16] Según se informa en su propia página web, la plataforma *"permite a los pacientes almacenar información de salud desde varias fuentes diferentes, acceder a una variedad de aplicaciones relacionadas con la salud y el estado físico, descargar datos de dispositivos de salud y estado físico, y compartir información de salud con las personas de confianza*". Disponible en: https://www.healthvault.com/es/es-US/providers

[17] Entre ellas, Walgreens, Quest Diagnostics o Longs Drugs según SÁNCHEZ OCAÑA, A. en *Desnudando a Google*, Deusto, 2012.

y de acuerdo con el artículo 17.4 la responsabilidad de custodiar las historias clínicas recae en la dirección del centro sanitario, la guarda de los datos de salud almacenados en un dispositivo insertado en un cuerpo humano corresponderá en cambio a la empresa que incorpora el chip a su sistema de cloud computing. Es decir, asumirá una responsabilidad en la custodia de la documentación asistencial generada por los profesionales sanitarios, responsables de su creación; de lo que se deduce que le corresponderá igualmente garantizar su mantenimiento, seguridad, gestión y confidencialidad y aplicar las medidas de seguridad que prevé el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal[18].

En cuanto a la conservación, uno de los principales problemas que puede plantear que la gestión y custodia no se lleve a cabo por el propio centro sanitario sino por una empresa especializada en la materia y regida por leyes estadounidenses, no sometida por tanto a nuestra normativa española, es en relación con el periodo mínimo de conservación de la historia clínica[19]. Estas empresas se suelen reservar en sus condiciones de uso la posibilidad de suspender el servicio en cualquier momento, eliminando nuestra información cuando quieran, y en consecuencia no garantizan su conservación indefinida o al menos durante el tiempo establecido legalmente. A título de ejemplo, Google decidió suspender en enero de 2012 su servicio, dando un año adicional para que los usuarios pudieran recuperar sus datos y transcurrido el cual fueron borrados de forma irrevocable y permanentemente[20].

No cabe duda de que el legislador estaba pensando, al atribuir la responsabilidad de la conservación y custodia de las historias clínicas, en que las mismas se almacenaban en el centro sanitario. En todo caso, el marco futuro

[18] 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 que en sus artículos 89 a 104 contempla las medidas de seguridad aplicables a ficheros y tratamientos automatizados

[19] El artículo 17.1 de la Ley 41/2002, bajo la rúbrica *"La conservación de la documentación clínica*" dispone que los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial; si bien, algunas leyes autonómicas establecen plazos más elevados.

[20] Los términos de uso del servicio Google Health están accesibles aún en http://www.google.com/intl/en_us/health/terms.html y la decisión empresarial de suspensión del servicio se encuentra disponible en https://www.healthvault.com/es/es-US/providers

adecuado sería aquel en que esas actividades se externalizan, siendo asumidas por la entidad ajena al centro sanitario a la que se ha realizado el encargo, aunque seguirá siendo responsable directa de su conservación y custodia su dirección o el órgano que a nivel estatal o europeo se cree ad hoc y/o se determine con esa finalidad, debiendo de estar además la información necesariamente almacenada en un servidor de Internet dedicado de su titularidad. Así pues, no sólo se daría sobrado cumplimiento a la previsión contemplada expresamente en el artículo 15.4 de la Ley básica al afirmar *"La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial",* sino que se haría realidad y a nivel europeo un propósito mucho más ambicioso que aquel que el legislador perseguía en su Disposición Adicional Tercera[21]: la implantación de un sistema de compatibilidad que posibilite el uso de la historia clínica del paciente ya no sólo por los centros asistenciales de España si no por los de toda Europa.

En este sentido, hay que señalar que el artículo 12 de la Ley 15/1999, prevé la figura del encargado del tratamiento bajo la rúbrica "*acceso a los datos por cuenta de terceros*"[22]. Conforme a dicho precepto, a los datos contenidos en la historia clínica podrá acceder la persona física o jurídica subcontratada para el cumplimiento de los fines encomendados, sin necesidad del previo consentimiento del paciente. Ahora bien, que no se necesario su consentimiento no significa que no haya de ser informado de esa comunicación de sus datos a un tercero[23].

---

[21] La Disposición Adicional Tercera de la Ley 41/2002, bajo la rúbrica "*Coordinación de las historias clínicas*" establecía un mandato al Ministerio de Sanidad y Consumo para que en coordinación y con la colaboración de las Comunidades Autónomas competentes y la participación de todos los interesados implantase *"un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición."*

[22] El artículo 3 g) de la Ley define encargado del tratamiento como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento"*, esto es, es la entidad que trata los datos por encargo del responsable del tratamiento.

[23] Dispone además el artículo 12 que esa relación debe estar regulado en un contrato bien por escrito o en otra forma que permita acreditar la celebración y su contenido y estableciéndose

Por lo que hace al acceso de los datos sanitarios, en primer lugar, el artículo 18.1 de la Ley básica establece el derecho que tiene el paciente a acceder a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella, reconocimiento que ha de completarse con su derecho de acceso que la Ley 15/1999 como interesado le reconoce a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Si bien, en el ejercicio de este derecho la Ley 41/2002 hace unas reservas señaladas en el apartado 3 del artículo 18, de manera que el paciente puede tener acceso a la totalidad de los datos integrados en la historia clínica salvo a aquellos que en interés terapéutico del paciente sean recogidos de terceras personas y afecten a su confidencialidad, y a las anotaciones subjetivas de los profesionales participantes en su elaboración si se oponen.

Como se puede deducir, la implantación del chip permitirá que los pacientes tengan acceso de inmediato a su historia clínica mediante la lectura del código de identificación de su chip a través de su dispositivo móvil, exonerando a los centros sanitarios de garantizar la observancia de ese derecho, y dejando al mismo tiempo sin efecto el plazo temporal de los doces meses para que el titular pueda volver a ejercitarlo[24]; pero al mismo tiempo puede suponer un atentando contra la intimidad de terceros. Esta polémica quedaría resuelta otorgándole al paciente un perfil de acceso, de fácil y rápida lectura, que asegure una limitación a esa determinada información reservada y contenida en su historia clínica y a la que sí tendrán acceso los profesionales, dotados de perfil con acceso y control para modificar toda la información. Con esta opción se consigue así un equilibrio adecuado entre los intereses en conflicto y se da solución al mismo tiempo a otro supuesto conflictivo cual es la limitación del derecho a la información sanitaria del paciente por la existencia, a

---

que el encargado del tratamiento se obliga a tratar esos datos siguiendo las instrucciones del responsable y no para fines distintos. Igualmente y atendiendo al carácter sensible y confidencial de esos datos, el encargado no podrá comunicarlos a otras personas y cumplida la prestación los mismos deberán ser destruidos o devueltos a su responsable.

[24] El artículo 15 de la Ley 15/1999 establece que el derecho de acceso "sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

criterio del facultativo, de un estado de necesidad terapéutica, previendo en atención a razones objetivas que el conocimiento de su propia situación puede perjudicar gravemente a su salud; circunstancias de las que se debe de dejar constancia en la historia clínica. No obstante, hay voces que ya apuntaron que esta previsión debe ser desterrada[25].

Por último, podría plantearse la posibilidad de conceder al interesado ejercer directamente su derecho de rectificación reconocido en el artículo 16 de la Ley 15/1999 para la corrección de datos inexactos o incompletos, previa verificación de su identidad a través de sistemas de acreditación como la firma electrónica, debiendo limitarse a los datos identificativos (nombre, apellidos, documento nacional de identidad o similar) y de domicilio incluidos en la historia clínica[26].

III.2. ¿Invasión a la intimidad?

En otro orden de cosas, el respeto a la intimidad es un derecho que podría quedar en entredicho con una regulación que impusiese de forma obligatoria la implantación del chip subcutáneo en humanos y es que a pesar de considerar que no podía ser afín a un *wearable*, sí que se encuentran coincidencias con los peligros y riesgos que pueden derivarse de su uso, así como su injerencia en el derecho a la intimidad y privacidad de los usuarios[27].

---

[25] DE MIGUEL SÁNCHEZ, N., «Intimidad e historia clínica en la nueva 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 *Revista Española de Derecho Administrativo,* nº 117, 2003, pág. 20. La autora percibe que el peligro que se deriva de esta excepción reside en la adopción de actitudes que suponga un retorno al paternalismo médico, algo que ha de ser totalmente desterrado y que se encuentra en clara contradicción con el espíritu general de la Ley, impulsora de la autonomía del paciente.

[26] Sobre este punto, se ha sostenido que ese derecho se debe ampliar a otros datos de salud conocidos por el paciente, no demasiado técnicos y de cuya no veracidad tuviera constancia. En este sentido, SERRANO PÉREZ, Mª.M., «La protección de los datos sanitarios. La historia clínica» en *Seminario sobre Protección de Datos*, Ciudad Real, Universidad de Castilla-La Mancha, 9 y 10 de noviembre de 2005. Disponible en: https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf.

[27] Sobre los riesgos de los wearables para la privacidad de las personas, ver Dictamen conjunto sobre internet de las cosas, aprobado por las autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29). La elaboración del documento fue liderado por la

En este sentido, y por la mayor o menor incidencia que pueden tener en la intimidad de las personas, hemos de atender a la clasificación realizada por el Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías de la Comisión Europea[28], que distingue tres tipos de chip; uno de solo lectura similar al que hoy día se les inserta a los animales, otro de lectura/escritura y un tercer chip con función de localización y posibilidad de tratamiento de datos por parte de terceros, como el fabricante del soporte y que entroncaría las funciones del chip de lectura/escritura.

Retomando la cuestión relacionada con los peligros que se han puesto de manifiesto por las autoridades europeas, debemos señalar que la implantación de un chip -no sólo con funciones de lectura/escritura, sino que permita la geolocalización del portador- unido al registro de información sobre sus hábitos y estilos de vida o datos relativos a la actividad física y el deporte realizado, a pesar de que no se trate de datos de los denominados especialmente protegidos, pueden acabar proporcionando a terceros ajenos al tratamiento información inferida acerca de la salud del individuo. Igualmente, si al chip subcutáneo se le atribuye la posibilidad de poder de control sobre dispositivos en el ámbito doméstico, también conocida como tecnología domótica, las autoridades advierten que pueden quedar al descubierto y revelarse detalles de la forma de vida y los hábitos personales y familiares[29]. Situación que se traduciría, si esta vigilancia potencial llegara a producirse, en poder controlar la forma en la que las personas se comportan en la vida real y en una clara y sistemática violación de su intimidad.

Asimismo, más allá de análisis directos en los patrones de comportamiento de los seres humanos, las autoridades muestran su preocupación precisamente en la posible pérdida de control sobre la difusión de los datos personales, ya que *"al aumento de la cantidad de datos generados hay que sumar las posibilidades que existen para combinarlos y analizarlos de forma cruzada, obtener nuevos datos sobre*

Agencia Española de Protección de Datos junto con la Autoridad francesa (CNIL). Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[28] Vid. *Aspectd Éthiques des implants TIC dans le corps humain*.

[29] Así se ha hecho saber en Vid. Nota Informativa "*Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre internet de las cosas*".

los originalmente solicitados y utilizarlos para usos secundarios o no al tratamiento inicial".

Por último, podemos señalar como otro riesgo inherente al chip el susceptible de ser clonado[30].

III.3 Libertad religiosa versus El número 666 de la bestia

Los rumores que durante meses circularon por internet de una futura reforma sanitaria que, por razones de salud y seguridad, supondría con carácter obligatorio la implantación de un chip subcutáneo en el cuerpo de todos los estadounidenses y europeos, generó un debate muy intenso. Su repercusión se ha dejado sentir en determinados cristianos que han manifestado que supondría un atentado a su derecho fundamental a la libertad religiosa[31], al advertir en el chip el número 666, número del nombre de la bestia, tradicionalmente identificado con Satanás y el Anticristo y que tiene su origen en el libro de las *Relevaciones* o *Apocalipsis de San Juan*[32].

El origen de esta negativa está al parecer en que "*estos chips pueden tener 34 billones de combinaciones únicas de códigos de identificación individual, más que suficiente para permitir asignar un código único a cada ser humano sobre la Tierra, utilizando tres entradas de seis cifras (666)*"[33].

[30] Como informa la agencia de noticias de Reino Unido Reuters en su blog, su vulnerabilidad supuestamente quedó demostrado en una conferencia celebrada en la ciudad de Nueva York en la que dos hackers demostraron a los asistentes la clonación de un chip RFID, dejando al descubierto que la tecnología de VeriChip no está blindada a posibles copias de sus dispositivos. Disponible en: http://blogs.reuters.com/blog/archives/1897

[31] Artículo 16 Constitución Española, desarrollado por Ley Orgánica 7/1980, de 5 de julio, de libertad religiosa.

[32] En este sentido, OLIVARES, C. «Elementos para descifrar el 666: una propuesta», DavarLogos, vol. 8, nº 1, 2009, págs. 31-58, al tratar de establecer la relación de la marca con el número de la bestia señala que *"El número 666 (Ap 13:18) está inmerso en el relato que describe el surgimiento y el accionar de la bestia que sube de la tierra (13:11-18)".*

[33] Diario La Capital, Agentina. Disponible en http://archivo.lacapital.com.ar/2004/07/04/candi.shtml.

Pensemos así en la confrontación entre el derecho de libertad religiosa y el derecho a la salud que se suscitaría cuando para su protección se aprobase una previsión legal expresa que faculte esa intervención corporal.

En cualquier caso, el ejercicio del derecho de libertad religiosa tiene como límite específico, entre otros, la salvaguardia de la salud, elemento constitutivo del orden público protegido por la Ley en el ámbito de una sociedad democrática[34] y así lo declaró el Tribunal Constitucional en su Auto número 369 de 20 de junio de 1984 al afirmar que esta libertad "tiene como límite la salud de las personas".

En conclusión, al ser la salud un límite que la Constitución ha impuesto expresamente al configurar el derecho de libertad religiosa y con el fin de preservar ese otro derecho fundamental reconocido, podría servir de argumento a nuestro legislador para hacerla ceder.

IV. BIBLIOGRAFÍA

- ALBRECHT, K., *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move,* foreword by bruce Sterling, wired.com, 2005.
- ALBRECHT, K., Synopsis of “Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006"
- CODÓN HERRERA, A., «La historia clínica: concepto, normativa, titularidad y jurisprudencia» en *Autonomía del paciente, información e historia clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, 2004, págs. 146-156.
- DE MIGUEL SÁNCHEZ, N., «Intimidad e historia clínica en la nueva 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 *Revista Española de Derecho Administrativo*, nº 117, 2003, págs. 9-30.
- DOMÍNGUEZ LUELMO, A., Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002, de 14 de noviembre, sobre derechos del

[34] Vid. Art. 3.1. Ley de libertad religiosa.

paciente, información y documentación clínica. Editorial Lex Nova, diciembre 2007.

- GARCÍA COSTA, F.M, «Los límites de la libertad religiosa en el derecho español», en *Díkaion: Revista de Actualidad Jurídica,* nº 16, 2007.
- OLIVARES, C. «Elementos para descifrar el 666: una propuesta», DavarLogos, vol. 8, nº 1, 2009, págs. 31-58.
- SÁNCHEZ OCAÑA, A. en *Desnudando a Google*, Deusto, 2012.
- SÁNCHEZ CARO, J., y ABELLÁN F., «Derechos y deberes de los pacientes. Ley 41/2002 de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas». Editorial Comares, Granada, 2002.
- SERRANO PÉREZ, Mª. M., «La protección de los datos sanitarios. La historia clínica» en *Seminario sobre Protección de Datos*, Ciudad Real, Universidad de Castilla-La Mancha, 9 y 10 de noviembre de 2005.
- VIDAL FUEYO, Mª, C., «Cuando el derecho a la libertad religiosa colisiona con el derecho a la educación» en *Revista Jurídica de Castilla y León*, nº. Extra 1, 2004, págs. 299-338.