Robótica en el ámbito sanitario y de los cuidados: implicaciones para la privacidad y la protección de datos*

Medical and Care Robots: Privacy and Data Protection Implications

Mª Belén Andreu Martínez

Universidad de Murcia (España)
beland@um.es

ISSN 1989-7022

Resumen: La tendencia al incremento del uso de robots en el ámbito de la salud y los cuidados personales implica importantes desafíos. Uno de ellos será la gestión de datos que se van a recoger, generar y compartir en este contexto. El presente trabajo aborda algunas de las principales cuestiones relacionadas con la privacidad y protección de datos de los usuarios de estos servicios. Se establece un marco de referencia en base al Reglamento europeo de protección de datos personales y las líneas de actuación que, para el ámbito jurídico y ético, se han ido fijando por las instituciones europeas en esta materia.

Palabras clave: privacidad, protección de datos, robótica, salud, cuidados personales

Abstract: The increasing tendency to use robots in health and personal care services will imply important challenges. Data management that will be collected, generated and shared will be one of them. This work addresses some of the main issues involved in the privacy and data protection for users of these services. It establishes a reference framework, based on the European Regulation of personal data protection and on the guidelines that, for the legal and ethical scope, have been set by the European institutions in this matter.

Keywords: privacy, data protection, robotics, health, personal care

Mª Belén Andreu Martínez: "Robótica en el ámbito sanitario y de los cuidados: implicaciones para la privacidad y la protección de datos", en Mario Toboso, Manuel Aparicio y Daniel López: Debate: Ética, robótica y tecnologías asistenciales
***ILEMATA**, Revista Internacional de Éticas Aplicadas*, nº 30, 79-92

1. La robótica en el contexto de la UE y su delimitación

Conviene, con carácter previo, hacer algunas precisiones acerca del contexto general en el que se enmarca la robótica a nivel europeo, así como desde el punto de vista conceptual. La inteligencia artificial y la robótica está siendo objeto de atención creciente en los últimos años. El impacto que ya se observa y que puede tener en el futuro a muy distintos niveles (social, económico, ético, en derechos humanos…), ha hecho que también se empiece a abordar desde el punto de vista jurídico y se plantee la necesaria adaptación normativa. Preocupan aspectos como su capacidad creciente de actuación autónoma, la falta de transparencia, los resultados en gran medida imprevisibles, y los problemas asociados a su control o la responsabilidad, entre otros. Las iniciativas que han ido surgiendo, centrándonos en el ámbito europeo, provienen de organismos como el Parlamento y la Comisión europea, el Consejo Económico y Social Europeo o el Consejo de Europa, así como de grupos de expertos creados en el seno de estas instituciones. En ellas se contienen recomendaciones, directrices y principios básicos que deben guiar el desarrollo de las políticas en este ámbito, incluido su reflejo en una futura regulación o adaptación normativa, aunque también con especial incidencia en el desarrollo ético de estas tecnologías.

* Este trabajo se enmarca en el proyecto "Datos de salud: claves ético-jurídicas para la transformación digital en el ámbito sanitario" (Fundación Séneca-20939/PI/18).

Received: 27/04/2019
Accepted: 09/05/2019

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

En concreto, específicamente destinadas a la robótica, básicamente se encuentra la Resolución dictada por el Parlamento europeo en febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (Parlamento europeo, 2017), en la que se solicitaba a la Comisión la presentación de una Directiva en la materia, y que se acompañaba de un código de conducta ética para ingenieros en robótica, un código deontológico para los comités de ética de la investigación y licencias para diseñadores y usuarios. En otros informes, directrices o resoluciones se aborda de forma conjunta las cuestiones que plantean la robótica y la inteligencia artificial (IA), o se centran de forma prioritaria en esta última. De hecho, el objetivo declarado es la creación de una IA "made in Europe".

En esta línea ha asumido un papel muy activo la Comisión europea, que presentó en abril de 2018 todo un paquete de medidas. Por un lado, la Comunicación sobre Inteligencia artificial para Europa[1], con un enfoque basado en tres pilares, siendo uno de ellos el establecimiento de un marco ético y jurídico apropiado[2]. Para su consecución, creó en junio de 2018 un grupo de expertos en IA (High-Level Expert Group on Artificial Intelligence, IA HLEG), que ha publicado ya las mencionadas directrices éticas (Ethics Guidelines for Trustworthy AI, de 8 de abril de 2019). Por otro lado, y en la medida en que el acceso a los datos constituye un elemento esencial para el desarrollo de esta tecnología, a través de una serie de medidas que pretenden impulsarlo y que se enmarcarían dentro de la llamada "economía de los datos" que se quiere implantar en Europa[3], y entre las que se encuentra la aprobación del Reglamento (UE) 2018/1807 del Parlamento europeo y del Consejo, de 14 de noviembre de 2018, sobre libre circulación de datos no personales. Este último reconoce como principales fuentes de estos datos no personales el internet de la cosas, la inteligencia artificial y el aprendizaje automático (cdo. 9). Esta política de acceso a los datos se extiende además al ámbito sanitario, que constituye uno de los ejes prioritarios en el ámbito de la transformación digital, con la finalidad de conseguir una asistencia sanitaria más enfocada a la promoción de la salud, la prevención y centrada en el paciente[4].

Por su parte, el Parlamento europeo ha aprobado en febrero de 2019 la Resolución sobre una política industrial global europea en materia de inteligencia artificial y robótica (Parlamento europeo, 2019), en la que se destaca, entre otras muchas cuestiones, el enfoque centrado en el ser humano que deben adoptar estas tecnologías. Como se puede comprobar, frente a un inicial impulso del Parlamento europeo para regular ciertos aspectos de la robótica, el interés principal se ha ido centrando en el desarrollo de un marco jurídico y ético para la IA y en el acceso a los datos.

En relación con esto también encontramos dificultades a nivel conceptual. IA y robótica son fenómenos vinculados, aunque como sabemos, no todo robot en un sentido amplio incorpora IA y ésta puede operar únicamente a nivel lógico, típicamente un chatbot (Vida Fernández, 2018, 208-209). Un primer problema que se suele señalar cuando se aborda el tema de los robots es que no existe una única definición que pueda aplicarse a la multitud de fenómenos que se suelen incluir y que recoja características comúnmente aceptadas para los mismos (Palmerini, 2017; Santos González, 2017)[5]. Aunque la corporeidad o el elemento físico es un rasgo característico, el término puede referirse a realidades muy distintas, que se aplican en múltiples ámbitos y con muy diversas funciones: robótica industrial, automóviles sin conductor, drones, robots quirúrgicos, asistenciales, dispositivos implantables en el cuerpo… En un sentido más estricto, se ha identificado el robot con un dispositivo mecánico capaz de

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

responder al paradigma sentir-pensar-actuar, esto es, capaz de recoger datos mediante sensores (sentir), procesar estos datos para decidir cómo responder (pensar) y realizar acciones actuando en el entorno, reflejando dichas decisiones, normalmente en función de objetivos prefijados (actuar); y solo eventualmente tendría las capacidades de comunicación con un operador, otros robots o una red externa (Barrio Andrés, 2018, 69-70; Palmerini, 2017, 65)[6]. Esto excluiría del concepto de robot a programas informáticos (aunque permitan interactuar con el entorno a través de interfaces de usuario). No obstante, los límites entre IA y robótica no siempre son nítidos (ni se sabe si evolucionarán o no hacia una mayor convergencia, Balkin, 2015), y los problemas que presentan desde el punto de vista ético o jurídico puede ser en parte comunes, aunque la robótica presenta consecuencias específicas derivadas de su interacción con el medio. Partiendo de esto, en este trabajo nos vamos a centrar específicamente en algunos tipos de robots aplicables en el ámbito sanitario y asistencial, y la tipología de datos que pueden recabar, para tratar algunos aspectos que se plantean desde el punto de vista de la privacidad y la normativa de protección de datos personales.

2. Robótica en el ámbito sanitario y de los cuidados y tratamiento de datos

Como hemos apuntado, la tipología de robots es muy diversa, y según el elemento al que se atienda (funcionalidad, interacción con el hombre…) se puede distinguir entre robots industriales, de servicios, autónomos o no autónomos, etc. Partiendo de la autonomía y el elemento de corporeidad, se ha desarrollado, especialmente en el ámbito de la sanidad y los cuidados, la llamada robótica inclusiva (Sánchez-Urán Azaña, Grau Ruiz, 2018, 10-11). No obstante, en el ámbito de la salud, las funciones que pueden llegar a desempeñar los robots son muy variadas (en cirugía, farmacia, rehabilitación, robots hospitalarios, etc.). Se han señalado tres grandes ámbitos de aplicación de la robótica en este campo, a los que también se refiere la Resolución con recomendaciones sobre normas de derecho civil para la robótica (García Portero, 2018, 207-210; Parlamento europeo, 2017): el quirúrgico, el rehabilitador/protésico y el asistencial o de cuidados.

El que se encuentra más generalizado a día de hoy es el de los robots quirúrgicos, que dotan al cirujano de mayor precisión, con ventajas para el paciente (en tiempos de operación o recuperación, por ej.), siendo uno de los más conocidos el robot Da Vinci[7]. Estos robots pueden almacenar, entre otros, el historial de la intervención realizada o las constantes vitales en relación con la actividad quirúrgica llevada a cabo; si bien *a priori* no plantean especiales cuestiones a efectos de este trabajo, más allá de las relativas al tratamiento de datos en el ámbito de la asistencia sanitaria. Donde se esperan los mayores avances y en donde se plantean los principales interrogantes es a propósito de los robots para rehabilitación y, especialmente, para el cuidado y asistencia. Dentro de los primeros encontramos una amplia gama, como los destinados a la rehabilitación de funciones corporales dañadas o la sustitución de miembros, la rehabilitación cognitiva y también se incluirían aquí los exoesqueletos[8] u otros elementos que pueden llevarse o implantarse en el cuerpo y, en su caso, las prótesis biónicas avanzadas, que preocupan en particular al Parlamento en la mencionada resolución, por cuanto pueden modificar la concepción en torno al cuerpo humano sano (e introducen el peliagudo tema de la mejora humana; Parlamento europeo, 2017).

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

Un ámbito prioritario, dados los retos que plantea, entre otros, el envejecimiento de la población, es el de los robots de cuidado y asistencia. En las directrices éticas para una IA confiable (IA HLEG, 2019) se señala precisamente como uno de los ámbitos clave para el desarrollo de la IA y la robótica, la asistencia a cuidadores, el apoyo en el cuidado de personas mayores o el monitoreo en tiempo real de pacientes. Aunque en un primer momento pudieron surgir como apoyo al personal sanitario en tareas básicas o repetitivas (como limpieza, desinfección, reparto de medicinas, control de temperatura… García Portero, 2018, 208), en la actualidad una de sus principales funcionalidades es el cuidado de personas mayores, con discapacidad o con determinadas enfermedades, superando el marco estrictamente sanitario[9]. La variedad, a su vez, dentro de los robots de asistencia y cuidados personales es muy amplia. En la ISO 13482:2014, específica para este tipo de robots, se hace referencia a robots con la finalidad de transportar personas y a robots asistentes físicos, que ayudan a realizar determinadas tareas, proporcionando un suplemento o aumentando las propias capacidades (y que incluirían los que no se sujetan al cuerpo y los que sí lo hacen – como exoesqueletos o wearable suits-). Hay que tener en cuenta, además, que estos últimos también se podrían utilizar con función rehabilitadora, tal y como hemos señalado anteriormente. Y robots de servicio móvil que, a diferencia de los anteriores, sí interactúan con la persona, y que realizan una tarea para ésta (manejar objetos o intercambiar información)[10]. Aunque los dos primeros señalados no parecen presentar *a priori* especiales problemas desde el punto de vista de la protección de datos, ya que están destinados a tareas concretas, sin embargo pueden llegar a captar bastante información (personal y no personal). Por ejemplo, los de transporte, sobre comportamiento del usuario (horarios, citas, etc.) y sobre el entorno. En el caso de los asistentes físicos, recogen los movimientos del paciente o controlan el uso que se hace del dispositivo para que éste pueda funcionar, pero también con posibilidad de acceso y control por parte del personal sanitario en contextos de rehabilitación. Y, en particular, respecto de los integrados en el cuerpo (exoesqueletos) datos médicos (ej. enfermedades) o relacionados con la condición física de la persona y, eventualmente también, datos biométricos, para una mejor personalización y simbiosis con ésta (Fosch Villaronga, 2017). Pero, sin duda, los que pueden llegar a captar mayor información, hasta el punto de poder convertirse en una vigilancia continua, son los que se tienen una finalidad de asistencia social (cuidador), incluyendo todo tipo de datos sobre el estilo de vida o hábitos de la persona en su vida diaria. En este sentido, se podrían tratar, entre otros, datos de geolocalización, monitorización de constantes vitales, gestión de alarmas médicas, monitorización para determinar si el paciente toma la medicación prescrita, reconocimiento de voz, grabación de sonidos, captura rápida de imagen para hacer streaming de vídeo, recopilación de información sobre las actividades observables del usuario para monitorizar la ejecución del plan establecido, almacenamiento de la información a medida que el usuario la va dando a través del diálogo con el robot y, eventualmente, podría incorporarse en un futuro un sistema de computación afectiva (ej. análisis de la gestualidad de la persona de cara al reconocimiento, gestión y generación de emociones). Por otra parte, también existe la posibilidad de almacenamiento en la nube de estos datos y de que estos robots interactúen con otros objetos (o con el Internet de la cosas) para compartir datos (García Portero, 2018, 224). Con todo, no hay que perder de vista que, en España, tanto este tipo de robots como los anteriores no se encuentran aún generalizados y, en muchos casos, estamos hablando de prototipos en fase de experimentación o de posibilidades que los dispositivos actuales aún están lejos de hacer.

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

El Parlamento reconoce que el mayor uso de sensores en el ámbito de la robótica ha ampliado su campo de aplicación a la prestación de los cuidados, permitiendo obtener servicios más personalizados, lo que también genera datos más pertinentes (Parlamento europeo, 2019). Como hemos visto, estos van desde datos médicos, de localización, de estilo de vida y hábitos, biométricos o comportamentales, entre otros. Dada la gran variedad de robots, de contextos y de tipología de datos a los que nos hemos referido, y las limitaciones propias de un trabajo de este tipo, vamos a detenernos a continuación en algunas de las cuestiones que se plantean desde el punto de vista de la privacidad y de la normativa de protección de datos personales.

3. La incidencia del RGPD en los datos recabados en la robótica sanitaria y asistencial

La primera cuestión que se plantea, de cara a la aplicación del Reglamento (UE) 2016/679, de 27 de abril de 2016, de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales (RGPD), es la calificación como datos personales de la información captada en los contextos anteriormente descritos. Y un segundo paso será su posible inclusión en ciertas categorías que cuentan con una especial protección, como los datos de salud o los datos biométricos. En esto, como sabemos, el RGPD ha optado por un carácter expansivo tanto del concepto de dato personal, como de la categoría de datos de salud, lo que permite un amplio marco de aplicación de esta norma.

Respecto al concepto de dato personal, se sigue considerando como tal toda información sobre una persona física identificada o identificable[11]. La clave para considerar aplicable o no la normativa de protección de datos sigue estando en determinar si es posible una identificación indirecta de la persona (teniendo en cuenta que se hace una interpretación bastante extensiva de esta posibilidad) y en si se ha procedido a una anonimización de los datos (lo que plantea no pocas dificultades, especialmente en contextos de captación masiva de datos e interconexión entre objetos). Esta cuestión es la que se trasluce, por ejemplo, en la Decisión de 8 de febrero de 2017 del Consejo de Estado francés, en la que se confirma la no autorización por parte de la CNIL (Commission nationale de l'informatique et libertés), por insuficiente anonimización de los datos, del proyecto presentado por la empresa JCDecaux France para computar el flujo de peatones en el barrio de la Défense de Paris[12]. Por ello, y aun cuando se aconseje proceder en la medida de lo posible a una anonimización de los datos recabados en el contexto de la robótica, habrá que poner especial cuidado en los riesgos de reidentificación. De ahí que deban adoptarse medidas dirigidas a tomar en cuenta y prevenir este riesgo, aspecto este último en el que se ha insistido como mecanismo de protección de las personas en contextos de *big data* (entre otros, Consejo de Europa, 2017). También el Reglamento (UE) 2018/1807 de 14 de noviembre de 2018, sobre libre circulación de datos no personales, prevé que, si los avances tecnológicos hicieran posible transformar datos anónimos en datos personales, debería aplicarse el RGPD (cdo. 9).

En cuanto a los datos de salud, el RGPD los define de forma bastante amplia (en especial, considerando 35; Beltrán Aguirre, 2017). Así, respecto a la tipología de datos que entrarían, no se refiere únicamente a los datos directamente relacionados con la salud de una persona en sentido amplio (salud física o mental), sino cualquier información sobre el estado de salud (Álvarez Rigaudias 2017, 173). Y, además, es independiente de la fuente de la que se obten-

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

gan, incluyéndose específicamente los dispositivos médicos (Alarcón Sevilla, Andreu Martínez, 2016); concepto que, para el Grupo de Trabajo del Artículo 29, debería interpretarse en sentido amplio, como cualquier dispositivo o aplicación que se utilizan en este contexto, con independencia de que tenga la calificación de "dispositivo médico" [13].

Ello permite dar cabida a los datos claramente relacionados con el estado de salud de la persona y que se puedan recabar en el marco de la robótica aplicada a la asistencia sanitaria y a los cuidados, pero eventualmente también otros que pudieran plantear más dudas, como los relativos al estilo de vida y bienestar (SEPD, 2015), que pueden ser objeto de tratamiento (ej. en la robótica asistencial), ya sea directamente o en combinación con otros dispositivos, en la medida en que acaben dando información sobre el estado de salud o riesgo para ella. En esta línea, el Grupo de Trabajo del Artículo 29, a propósito de la información que se capta o procesa por distintos dispositivos (sensores, wearables…), identifica tres tipos de datos que pueden considerarse o convertirse en datos de salud, ya que pueden acabar dando información sobre el estado o riesgo para la salud: datos claramente de carácter médico; datos en bruto de los sensores, que se pueden usar por sí mismos o combinándolos con otros para llegar a una conclusión sobre el estado de salud real o riesgo para ésta; y conclusiones extraídas sobre el estado de salud o riesgo de salud de una persona (sean exactas o no, e independientemente de que los datos de los que se extraigan puedan o no ser considerados de salud)[14]. Del documento del Grupo de Trabajo se pueden extraer algunas consideraciones de relevancia a la hora de calificar la información obtenida como dato de salud: no es suficiente con atender al carácter del dato en sí, sino que también hay que tener en cuenta el uso previsto, por sí solo o en combinación con otros datos; y otro elemento relevante sería el impacto que en la privacidad de la persona puede tener el tratamiento de los datos.

Junto a esta definición amplia de dato de salud, el RGPD incorpora la de datos biométricos, que, como hemos visto, también pueden tener cierto juego en este contexto (en robótica de asistencia social, eventualmente en el uso de exoesqueletos). Se consideran como tal los datos obtenidos por un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona, que permitan o confirmen la identificación única de dicha persona. Como se puede observar, no todo dato sobre dichas características es un dato biométrico, sino que es necesario que se haya obtenido a través de un procedimiento técnico específico destinado a obtener el dato a partir de las características del sujeto; y se refieren a características que permitan la identificación única o unívoca de la persona[15]. El RGPD cita como ejemplo la huella dactilar o la imagen facial; y el Grupo de Trabajo del Artículo 29 (Dictamen 3/2012) hace referencia a técnicas biométricas basadas en aspectos físicos y fisiológicos (comprobación de huellas digitales, reconocimiento del iris, facial de voz, análisis de retina…) y en aspectos comportamentales (análisis de la forma de caminar, de moverse, pautas que indiquen el pensamiento subconsciente de una persona…). Es precisamente esta vinculación directa con una persona la que justifica una protección reforzada. Y, en este sentido, aunque no se consideren datos de salud, comparten con estos ciertos aspectos de su régimen jurídico, como por ejemplo, las bases de legitimación de tratamiento (art. 9), a las que nos vamos a referir a continuación. En cualquier caso, más allá de que la información captada a través de sistemas robóticos pueda incluirse o no dentro de las categorías especiales de datos señaladas, la protección en contextos de especial riesgo se canaliza a través de los instrumentos que prevé ahora el RGPD dentro de la responsabilidad proactiva o las limitaciones a la elaboración de perfiles.

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

El consentimiento de la persona afectada es uno de los supuestos clásicos de legitimación del tratamiento de datos personales. En el RGPD éste conserva las características que se venían predicando de él (libre, específico, informado e inequívoco, con especial incidencia en este último, al haberse excluido los consentimientos por inacción o silencio). En el caso de datos biométricos y de salud, el consentimiento además debe ser expreso. El Parlamento europeo ha insistido en la necesidad de que un diseñador de IA o robótica siempre debe contar con un consentimiento consciente, claro e inequívoco y debe establecer los procedimientos para garantizar un consentimiento válido, debiendo recabarse con anterioridad a cualquier interacción hombre-máquina (Parlamento europeo, 2017, anexo y 2019, 129)[16]. Ello debería incluir, entre otros, una información clara sobre qué datos se recaban y cómo se utilizarán, para que pueda conocer el verdadero impacto en la persona del tratamiento que se realiza a través del robot (no olvidemos que el art. 13 RGPD incluye la información sobre decisiones automatizadas y elaboración de perfiles, así como la importancia y consecuencias previstas para el interesado); y debe preverse igualmente que el consentimiento puede ser retirado en cualquier momento. Aún así, no hay que perder de vista la dificultad de cumplir con los requisitos del consentimiento en este contexto y asegurar así su validez (en particular, respecto a la información o la libertad –que implica la posibilidad real de no prestar el consentimiento y la existencia de alternativas válidas[17], Dictamen 8/2014, Grupo de Trabajo del Artículo 29). De hecho, desde hace años, se viene señalando la insuficiencia del consentimiento como mecanismo de protección de la persona en el nuevo contexto tecnológico, entre otros, de captación y análisis masivo de datos (SEPD, 2015b; Cotino Hueso, 2017). De ahí que se insista más en el enfoque de responsabilidad proactiva que ahora incorpora el RGPD y, en general, en la necesidad de abordar esta materia desde un punto de vista más amplio, que incorpore el impacto ético y en derechos fundamentales, como señalaremos más adelante. El consentimiento, siendo un elemento que dota de licitud al tratamiento, pierde relevancia en favor de otras garantías.

Por otra parte, centrándonos en las categorías especiales de datos señaladas que pueden recabarse en el ámbito de la robótica médica y asistencial, hay que tener en cuenta que el RGPD prevé otras bases legítimas para su tratamiento (sin consentimiento del interesado) y que su configuración en contextos socio-sanitarios es ahora más amplia (Andreu Martínez, Pardo López, Alarcón Sevilla, 2017) [18]. De entre estas bases jurídicas podríamos destacar la relativa a la prestación de asistencia o tratamientos de tipo sanitario o social. Ésta legitimaría el tratamiento de datos de salud recabados a través de sistemas robóticos, pensando en una cada vez mayor penetración de estas tecnologías en el ámbito sanitario y social, siempre que se hagan en el marco de dicha asistencia y con los requisitos que establece el propio RGPD (que sea prestada por profesionales sanitarios, u otros, sujetos al secreto profesional o bajo su responsabilidad, y sobre la base de la normativa –sobre todo sanitaria[19]– o en virtud de un contrato con un profesional sanitario). Más difícil es, en cambio, incluir en esta causa de legitimación un posible tratamiento de datos biométricos en el marco de la utilización de sistemas robóticos, ya que la normativa legal se refiere únicamente a datos de salud (disposición adicional 17ª LOPDGDD). El RGPD también permite el tratamiento de datos (sin consentimiento) con fines de investigación científica (incluida la investigación en salud). Se trataría aquí de la utilización con este fin de datos obtenidos previamente en el marco de la utilización de sistemas robóticos, por ejemplo, para la asistencia sanitaria y social[20]; y requeriría el cumplimiento de los requisitos y garantías adicionales que establece el RGPD (proporcionalidad con la finalidad perseguida y garantías adecuadas para los derechos y libertades), y que han

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

sido concretadas por la LOPDGDD (pseudonimización, compromiso jurídico vinculante, evaluación de impacto, informe del comité de ética de la investigación…).

Por otra parte, dada la gran cantidad de datos que pueden llegar a recabarse en el ámbito de la robótica (incluidas las categorías especiales de datos antes señaladas) y el carácter invasivo en la intimidad que pueden llegar a tener, en particular la de asistencia social, cobran especial relevancia en este ámbito ciertos principios como el de proporcionalidad o la minimización de datos (dentro de la implementación de la privacidad desde el diseño y por defecto)[21]. Conforme al primero, habrá que hacer una evaluación de la necesidad y proporcionalidad del tratamiento de datos (tipo de tratamiento, mecanismos, categorías de datos…) con los objetivos que se pretenden conseguir. Y, en este sentido, habrá que determinar si el tratamiento es necesario para la finalidad o la necesidad que se pretende cubrir con él, si es proporcional a los beneficios que se esperan y si se puede conseguir ese objetivo con medios menos invasivos de los derechos de los interesados. Por lo tanto, situaciones de "mayor comodidad" no justificarían la introducción de mecanismos muy invasivos de la privacidad, de manera que la situación y necesidad real de la persona determinarán en qué casos procede la introducción de estos sistemas. Respecto al principio de minimización de datos, como sabemos, impone que el tratamiento sea efectuado de manera que se limiten a lo necesario para la finalidad tratada; por lo tanto, solo deberá tratarse o almacenarse la información necesaria, no toda la que se pueda recabar. Adicionalmente, podría acudirse a soluciones de pseudo (que no excluye la aplicación del RGPD) o anonimización cuando sea posible, con las advertencias antes realizadas acerca de los riesgos de reidentificación. Conforme al principio de privacidad por defecto, la obligación de tratar únicamente los datos necesarios se aplica tanto a la cantidad, como a la extensión del tratamiento, el plazo de conservación y el acceso a ellos. Esto último requiere precisar quién y cómo se accederá a los datos generados, por ejemplo, por un robot asistencial (limitaciones al acceso por parte de la empresa, tipos de datos a los que puede acceder el personal sanitario o la familia, con qué frecuencia o frente a qué eventos). Por otra parte, en cuanto a la conservación de los datos (y en relación con el derecho de cancelación), hay que prestar atención a la posible incorporación de datos generados en el ámbito de la robótica a la historia clínica de un paciente, en la medida en que la normativa sanitaria establece unos períodos mínimos de conservación que pueden llegar a ser amplios[22]. A priori, y conforme a lo previsto en la normativa sanitaria, solo debería incluirse la información trascendental para un conocimiento veraz y actualizado del estado de salud de una persona.

4. Más allá de la protección de datos: el derecho a la vida privada y la aproximación desde la ética

El cambio de paradigma que ha supuesto la aparición del análisis basado en el big data y la aparición de tecnologías que se nutren del análisis masivo de datos como la IA han puesto de relieve la necesidad de abordar la tecnología desde un enfoque más amplio, aspecto éste que ha sido impulsado, en primer lugar, desde el propio ámbito de la protección de datos personales. Un buen ejemplo de ello es el SEPD, que viene abogando en los últimos años por el desarrollo de una ética digital (SEPD, 2015b). El Consejo de Europa, en su reciente guía sobre protección de datos e IA (2019) así como en las directrices previas sobre big data (2017), también ha apostado por incorporar una visión más general para la protección de los

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

derechos fundamentales y libertades de los ciudadanos, que requiere tener en cuenta las implicaciones éticas y sociales del uso de los datos.

De ahí que se propongan medidas como la evolución hacia una evaluación del impacto ético, social y en la privacidad, y la utilización, para la adaptación de dicha evaluación a contextos más concretos, de "comités de ética ad hoc" (Consejo de Europa, 2017 y 2019; Mantelero, 2018), que deberían identificar los valores éticos que deberían ser protegidos cuando la evaluación de riesgo detecte un alto impacto en dichos valores por el uso de la tecnología. El Parlamento europeo también ha sugerido la creación de comités de ética sobre robótica en hospitales e instituciones sanitarias, que contribuyan a resolver las cuestiones éticas especialmente complejas relacionadas con el cuidado y tratamiento de los pacientes. En nuestro país, esta función podrían cumplirla los Comités de ética asistencial, que ya se encargan de estas cuestiones con carácter general en la asistencia sanitaria y que, además, lo hacen conforme a los principios de la bioética (que son los que el propio Parlamento propone seguir, aunque adaptados al ámbito de la robótica; Parlamento europeo, 2017).

Por otra parte, hay que tener en cuenta que la privacidad no se reduce a la protección de datos personales. Ciertamente el marco regulatorio de este último ha extendido su ámbito de aplicación en los últimos años hasta el punto de haber "fagocitado" en cierta medida otros derechos relacionados, como la intimidad o la propia imagen. La amplitud del concepto de dato personal y, sobre todo, el de tratamiento (junto a la "facilidad" de acceso al mecanismo de protección del derecho a través de la autoridad independiente de control) han facilitado este fenómeno y el solapamiento en los mecanismos de protección En cualquier caso, está claro que las situaciones que plantean ciertos robots de asistencia y cuidado inciden de manera muy especial en el derecho a la vida privada, derecho que incluye, además, múltiples facetas (física, espacial, mental…). Los robots asistenciales a personas enfermas, con discapacidad o mayores pueden tener como finalidad controlar el estado de salud, la toma de medicamentos, la posibilidad de caídas, etc. Pero igualmente pueden controlar otros aspectos de la vida cotidiana (actividad física, aseo, etc.). En la medida en que el robot puede ver, escuchar, percibir emociones y, en general, controlar todos los aspectos de la vida diaria de una persona (hasta el punto de estar sometida a una vigilancia continua), el espacio de intimidad de esta puede verse enormemente reducido hasta el punto de casi ser inexistente. Además, se plantea el problema adicional de que esto puede afectar también a terceros que se relacionen con esa persona, por lo que deberán adoptarse medidas adicionales para la protección de su intimidad (Palmerini et al., 2014, 191).

La causa de legitimación para la intromisión en este derecho ha sido tradicionalmente el consentimiento, por lo que éste constituye un elemento esencial para justificar situaciones que puedan suponer una vulneración de este derecho a través del uso de un robot de tipo asistencial. Aquí serían aplicables los tradicionales requisitos exigidos para la validez del consentimiento: competencia de la persona (debiendo prestarse los apoyos necesarios en el caso de personas con discapacidad, conforme al art. 12 Convención ONU de los derechos de las personas con discapacidad); que sea libre (por lo que la persona debe haber tenido la posibilidad real de rechazarlo, sin que ello le suponga un perjuicio; lo que entroncaría con el derecho de la persona a no usar este tipo de robots); e informado (la persona debe conocer, a través de la correspondiente información, el impacto que en la vida privada implica el establecimiento de un robot asistencial). No obstante, dada la intensidad descrita de la afectación al derecho

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

a la intimidad, se han propuesto garantías adicionales para reforzar la protección a través del consentimiento. Por ejemplo, el que el consentimiento para que un tercero pueda "acceder a nuestra intimidad" se limite a los casos de alertas o que, junto al consentimiento genérico para el establecimiento de un robot de este tipo fuera acompañado de consentimientos específicos en los casos en que un tercero quisiera realizar este tipo de control o vigilancia fuera de los momentos de urgencia o alerta (Nevejans, 2017, 890). También deberían establecerse mecanismos de desactivado o apagado, que evitaran los dispositivos siempre encendidos y situaciones de vigilancia permanente. Por otra parte, en relación con el establecimiento de robot asistenciales en el marco de programas de asistencia socio-sanitaria, habría que tener en cuenta lo establecido en el artículo 8.2 del Convenio europeo de derechos humanos, que permite la injerencia por parte de la autoridad pública en el derecho a la vida privada con los requisitos ahí establecidos: que la medida esté prevista en la ley, que tenga un fin legítimo (entre los que se encuentra la protección de la salud); y que sea necesaria en una sociedad democrática. Ello implica realizar la correspondiente ponderación entre el derecho a la vida privada y la protección de la salud de la persona, jugando un papel fundamental la proporcionalidad de la medida, a la que ya nos hemos referido anteriormente. Por lo tanto, habrá que tener en cuenta que la finalidad buscada no pueda conseguirse por otros medios menos invasivos de la intimidad de la persona y que, además, los mecanismos instaurados por defecto estén orientados a la protección de la intimidad[23].

Adicionalmente, la privacidad y la protección de datos han sido abordadas como principio ético en las guías y resoluciones a las que se ha hecho referencia al principio de este trabajo, entre ellas, las directrices éticas para una IA confiable (AI HLEG, 2019). Estas directrices no pretenden ser un mero listado de principios éticos, sino que también están dirigidas a dar una orientación sobre cómo aplicarlos. Y en este sentido, parten, en un primer nivel, de cuatro principios éticos (basados en los derechos fundamentales: respeto a la autonomía, prevención del daño, equidad y explicabilidad); recomienda, en un segundo nivel, la adopción de ciertos requisitos específicos (supervisión humana, la privacidad y gobierno de los datos, responsabilidad, transparencia…); y, como tercer nivel, se establece una lista de evaluación del cumplimiento de estos requisitos. Se ha querido, por tanto, dar un carácter "práctico" a estas directrices, concretando los principios éticos a nivel de listado de evaluación. No obstante, este enfoque instrumental basado en un listado de verificación ética ha sido expresamente rechazado desde otros sectores, en la medida en que "libera" de una reflexión o discusión ética más amplia (EDPS Ethics Advisory Group, 2018); y, por otra parte, también se puede producir un solapamiento con los requerimientos jurídicos. En el mencionado documento, el principio de privacidad y gobierno de los datos incluiría varios aspectos (que vendrían a constituir criterios básicos de referencia, independientemente de la regulación legal). Por un lado, el respeto a la privacidad y la protección de los datos, lo que significa asegurar la privacidad y la protección de los datos a lo largo de todo el ciclo de vida del sistema, lo que incluiría no solo la información proporcionada por el usuario, sino también la generada sobre el mismo como consecuencia de su interacción con el sistema; y que la información no se use para discriminar de manera ilegal o injusta. Por otro lado, la calidad e integridad de los datos, así como protocolos de acceso a los datos. En el listado de evaluación, se proponen una serie de cuestiones para identificar el cumplimiento de estos aspectos clave señalados. Aunque en el propio documento se reconoce la posibilidad de que medidas establecidas en este listado se superpongan con requerimientos legales, de manera que los procedimientos para garantizar el cumplimiento de estos requerimientos también pueden ayudar a un manejo ético de los

ISSN 1989-7022

datos. En última instancia, lo que se deja entrever es una falta de claridad acerca de cuál es el papel que debe jugar la ética en este ámbito.

Por lo demás, en el ámbito de la robótica, especialmente en la asistencial, la privacidad abordada desde un enfoque ético ha permitido un debate más amplio, no solo sobre el derecho a no ser "vigilado", sino también acerca de un elemento esencial en el ámbito sanitario y de la llamada "relación médico-paciente", como es el contacto humano. Esto se enmarcaría en el desarrollo como persona y la necesidad de las relaciones con otros seres humanos, y en el papel que debe cumplir un robot en el cuidado y qué funciones pueden delegarse, con fundamento en la dignidad humana[24]. En esta línea, en el Statement on Artificial Inteligence, Robotics and "Autonomus" Systems (EGE, 2018) se llama la atención sobre el debate acerca de la posibilidad de reconocer el derecho al contacto humano. Por su parte, el Parlamento europeo hace hincapié en el principio de autonomía supervisada de los robots (con base en el criterio señalado por el propio Parlamento de que la robótica debe complementar las capacidades humanas, no sustituirlas; Parlamento europeo, 2017) y, en general, en la influencia del desarrollo tecnológico en la relación médico-paciente y las nuevas coordenadas de esta relación en el siglo XXI, que no se debe ver perjudicada por el desarrollo de la robótica, sino más bien al contrario, servir de apoyo para una mejora de la calidad y eficiencia en la asistencia sanitaria. Y, a propósito de la robótica asistencial, destaca el contacto humano como uno de los elementos fundamentales de la atención a las personas.

Dilemata, año 11 (2019), nº 30, 79-92

Bibliografía

Alarcón Sevilla, V., Andreu Martínez, M. B. (2016). "La vulnerabilidad de los datos de salud en tecnología móvil". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 42, pp. 135-155.

Álvarez Rigaudias, C. (2017). "Tratamiento de datos de salud", en Piñar Mañas, J. L. (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Protección de Datos*. Madrid, Editorial Reus, pp. 171-185.

Andreu Martínez, M. B., Pardo López, M. M., Alarcón Sevilla, V. (2017). "Hacia un nuevo uso de los datos de salud". *Ius et Scientia*, 3(1), pp. 161-171.

Balkin, J. M. (2015). "The Path of Robotics Law", *California Law Review*, 5, pp. 45-60.

Barrio Andrés, M. (2018). "Del derecho de internet al derecho de los robots", en Barrio Andrés, M., *Derecho de los robots*. Madrid. La Ley-Wolters Kluwer, pp. 61-86.

Beltrán Aguirre, J. L. (2017). "Tratamiento de datos personales de salud: incidencia del Reglamento general de protección de datos", en Pérez Gálvez, J. F. (dir.), *Salud electrónica. Perspectiva y realidad*. Valencia, Tirant lo Blanch.

Calo, C. J. et al. (2011). "Ethical implications of using the paro robot with a focus on dementia patient care", 12th AAAI Conference on Human-Robot Interaction in Elder Care, pp. 20-24.

Calo, R. (2015). "Robotics and the Lessons of Cyberlaw", *California Law Review*, 103, pp. 513-564.

Consejo de Europa (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data.

Consejo de Europa (2019). Guidelines on Artificial Intelligence and Data Protection.

ISSN 1989-7022

Cotino Hueso, L. (2017). "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, 24, pp. 131-150.

Dominguez-Alcón, C. (2017). "Ética del cuidado y robots", *Cultura de los cuidados*, XXI, nº 47, pp. 9-13.

EGE (2018). European Group on Ethics in Science and New Technologies. Statement on Artificial Inteligence, Robotics and "Autonomus" Systems.

Fosch Villaronga, E. (2017). *Towards a Legal and Ethical Framework for Personal Care Robots. Analysis of Person Carrier, Physical Assistant and Mobile Servant Robot* (tesis doctoral). Universidad Autónoma de Barcelona. https://ddd.uab.cat/record/187696 (última consulta: 02.05.2019).

García Micó, T. G. (2014), "Litigación asociada a la cirugía robótica con el Da Vinci", *Indret*, 4, pp. 1-41.

García Portero, R. (2018). "Los robots en la sanidad", en Barrio Andrés, M., *Derecho de los robots*. Madrid. La Ley-Wolters Kluwer, pp. 203-228.

Greco, L., Mantelero, A. (2018), "Industria 4.0, robotica e privacy-by-desing", *Il Diritto dell'informazione e dell'informatica*, 6, pp. 875-900.

IA HLEG -High-Level Expert Group on Artificial Intelligence- (2019). Ethics Guidelines for Trustworthy AI.

Mantelero, A. (2018). "Ciudadanía y gobernanza digital entre política, ética y derecho", en De la Quadra-Salcedo, T., Piñar Mañas, J. L. (dirs.). *Sociedad digital y derecho*. Madrid, Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado, pp. 159-178.

Martínez Martínez, R. (2018). "Inteligencia artificial, derecho y derechos fundamentales", en De la Quadra-Salcedo, T., Piñar Mañas, J. L. (dirs.). *Sociedad digital y derecho*. Madrid, Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado, pp. 259-277.

Moreno, O. (2014). "Un robot de compañía para los ancianos. Proyecto Accompany". *I+S: Revista de la Sociedad Española de Informática y Salud*, 105, pp. 58-59.

Moreno, O. (2018). "Ingenieros y médicos construyen robots wearables juntos". *I+S: Revista de la Sociedad Española de Informática y Salud*, 131, p. 54.

Nevejans, N. (2017). *Traité de droit et d'éthique de la robotique civile*. Bordeaux, LEH Édition.

Palmerini, E. et al. (2014). "Guidelines on Regulating Robots", Robolaw Project. Deliverable D 6.2. http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf (última consulta: 01.05.2019).

Palmerini, E. (2017), "Robótica y derecho: sugerencias, confluencias, evoluciones en el marco de una investigación europea". *Revista de Derecho Privado*. Universidad Externado de Colombia, 52, pp. 53-97.

Parlamento europeo (2017). Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

Parlamento europeo (2019). Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088 (INI)).

Poullet, Y. (2010). «About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation», en Gutwirth, S. et al. (eds.). *Data Protection in a Profiled World*. Springer Science & Business Media, pp. 3-30.

Sánchez-Urán Azaña, M. Y., Grau Ruiz, M. A. (2018). *El impacto de la robótica, en especial la robotica inclusiva, en el trabajo: aspectos jurídicos-laborales y fiscales*. https://eprints.ucm.es/47523/ (última consulta: 02.05.2019).

Santos González, M. J. (2017). "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", *Revista Jurídica de la Universidad de León*, 4, pp. 25-50.

SEPD (2015). Supervisor Europeo de Protección de Datos. Opinion 1/2015 on Mobile Health. Reconciling technological innovation with data protection.

SEPD (2015b). Supervisor Europeo de Protección de Datos. Opinion 4/2015. Towards a new digital ethics. Data, dignity and technology.

Vida Fernández, J. (2018). "Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea", en De la Quadra-Salcedo, T., Piñar Mañas, J. L. (dirs.). *Sociedad digital y derecho*. Madrid, Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado, pp. 203-224.

Notas

1. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa, de 25 de abril de 2018, COM(2018) 237 final.

2. En relación con este aspecto, el objetivo de la Comisión ha sido proponer una guía sobre la interpretación de las actuales normas en materia de responsabilidad por productos defectuosos, unas directrices éticas sobre IA, e impulsar estudios y formular respuestas políticas a los desafíos planteados por AI en materia de responsabilidad, seguridad, Internet de las cosas (IoT), robótica, conciencia algorítmica, protección del consumidor o protección de datos.

3. Cfr. la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Hacia un espacio común europeo de datos", de 25.4.2018, COM(2018) 232 final (así como la previa: "Hacia una economía de los datos próspera", de 2.7.2014, COM(2014) 442 final).

4. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones relativa a la consecución de la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital, la capacitación de los ciudadanos y la creación de una sociedad más saludable, de 25 de abril de 2018 (COM(2018) 233 final).

5. Además, también se discute si deben o no establecerse unas características esenciales para los robots desde las cuales abordar la regulación de los problemas jurídicos que se planteen (Calo, 2015; Balkin, 2015).

6. El Parlamento europeo insta a la proposición de definiciones comunes europeas de sistema ciberfísico, autónomo, robot autónomo y sus distintas subcategorías, con base en ciertas características: capacidad de adquirir autonomía mediante sensores y/o intercambio de datos con su entorno y en análisis de dichos datos; capacidad de autoaprendizaje a partir de las experiencias e interacción (facultativa); soporte físico mínimo; capacidad de adaptar su comportamiento y acciones al entorno e inexistencia de vida en sentido biológico (Parlamento europeo, 2017).

7. En este tipo de robots existe un cierto consenso en cuanto a su clasificación, según el tipo de tecnología, las aplicaciones o el papel que desempeñan (García Micó, 2014; García Portero, 2018).

8. Vid., entre otros, el exoesqueleto Symbitron (Moreno, 2018).

9. La ISO 13482:2014, que contiene una definición de robots de cuidado personal, considera como tales los que llevan a cabo acciones dirigidas directamente a mejorar la calidad de vida, excepto para las aplicaciones médicas.

10. Un estudio exhaustivo de esta tipología y las implicaciones ético-legales en Fosch Villaronga, 2017. Realiza el autor un análisis crítico de las definiciones contenidas en la ISO y de las cuestiones que desde el punto de vista ético y legal no están contempladas y que podrían llevar a un incumplimiento de ciertas normas y desprotección de usuario. Entre otros aspectos, pone de relieve la doble posibilidad de utilizar algunos de estos robots en entornos asistenciales y fuera de ellos, y los problemas que a nivel legal plantea.

11. Y ello aunque la identificación de la persona pierda importancia en un contexto de captación masiva de datos como el actual, y en el que el procesamiento de datos y el perfilado puede afectar a los derechos de la persona, independientemente de que esté identificada (Poullet, 2010).

12. https://www.legalis.net/jurisprudences/conseil-detat-10eme-9eme-ch-reunies-decision-du-8-fevrier-2017/.

13. Annex-health data in apps and devices, 5.2.2015 (https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf). Se trata de una carta, que incluye como anexo este documento, en respuesta a la petición de clarificación de

ISSN 1989-7022

ISSN 1989-7022

Dilemata, año 11 (2019), nº 30, 79-92

la Comisión europea del concepto de datos de salud en relación con las aplicaciones sobre estilo de vida y bienestar.

14. Vid. el documento señalado en la nota anterior. Un ejemplo que pone de tratamiento adicional, en el sentido de datos de los que se extraen conclusiones sobre el estado de salud, es el análisis realizado en las redes sociales para detectar si las personas pueden sufrir de una depresión. Señala también específicamente los casos en que se usa cualquier tipo de información (de salud o no) para identificar riesgos de enfermedad, lo que puede ocurrir a menudo en investigación médica usando big data.

15. (Greco, Mantelero, 2018, 883-884). Señalan, como ejemplo, que la cara de una persona no es un dato biométrico, sino la imagen facial obtenida a través de un algoritmo de reconocimiento facial. Vid. también considerando 51 RGPD.

16. En el Statement on Artificial Inteligence, Robotics and "Autonomus" Systems (EGE, 2018) se remarca que tanto los robots físicos de IA como parte de IoT, como los softbots de IA que operan a través de internet, deben cumplir con la normativa en materia de protección de datos, haciendo hincapié en la necesidad de contar con el consentimiento (no deben recopilar ni difundir datos ni ejecutarse en conjuntos de datos para cuyo uso o difusión no obtuvieron el consentimiento informado). Sobre las condiciones para un consentimiento válido en contextos de big data, vid. también Consejo de Europa (2017).

17. Considerando 42 RGPD. Esto podría plantear dificultades en un contexto sanitario en ciertos casos, en los que la persona se pueda sentir obligada a dar su consentimiento o no darlo, o retirarlo le pudiera provocar un perjuicio (Martínez Martínez, 2018); y tampoco sería válido si hay una clara asimetría entre las posiciones de las partes, lo que ocurre generalmente cuando una de ellas es un poder público. (Comité Europeo de Protección de Datos. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. WP259 rev.01).

18. Para datos no sensibles, habría que acudir a las causas de licitud previstas en el art. 6 RGPD (eventualmente, podría tener aplicación aquí la relativa al tratamiento necesario para la ejecución de un contrato; y no parece que quepa la satisfacción de intereses legítimos del responsable, que difícilmente prevalecerá en la ponderación con los derechos y libertades de los interesados).

19. En cuanto a la base legal y normativa que permitiría el tratamiento de estos datos, arts. 9 y disposición adicional 17ª de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

20. La participación en un proyecto de investigación que incluya la utilización de robots sanitarios o asistenciales requiere el consentimiento del participante, lo que implica también la obtención del consentimiento para el tratamiento de los datos que se generen en el marco de la investigación, consentimiento que ahora puede ser "genérico" (considerando 33 RGPD; disposición adicional 17ª.2.a. LOPDGDD).

21. En este sentido, para la robótica en el ámbito de la industria 4.0, (Greco, Mantelero, 2018).

22. Cinco años en la normativa nacional (Ley 41/2002, 14 noviembre); plazo que puede ser más amplio en la normativa autonómica. Además, la Agencia española de protección de datos ha interpretado de forma bastante amplia este período de conservación para las historias clínicas (vid. por ejemplo, el procedimiento de tutela de derechos nº 670/2017).

23. A propósito del proyecto ACCOMPANY (robot de compañía para ancianos), se señala que si el robot está emplazado por las autoridades competentes (sistema de atención social o sanitario) en el domicilio de la persona mayor con la condición de que se notifiquen riesgos de seguridad, y el usuario está de acuerdo con esto, puede ser motivo para que el robot solicite ayuda, incluso si el usuario se opusiese (Moreno, 2014, 59).

24. Sobre la utilización como guía de los principios de la ética del cuidado para el uso de robots en el cuidado de personas, Dominguez-Alcón, 2017. En relación con el robot Paro y las implicaciones en relación con el contacto humano, Calo et al., 2011.