Entrevista con María Ángeles Egúsquiza Balmaseda*
Desafíos y soluciones en la protección de datos para consumidores de salud

Dimar Mejía Mendieta y Dayana Sofía Luján Sánchez**

doi: https://doi.org/10.26439/iusetpraxis2024.n59.7649

En su libro *Protección de datos: intimidad y salud*, usted analiza a profundidad los retos de la protección de datos en el ámbito de la salud. En su opinión, ¿qué desafíos legales persisten en la protección de datos médicos frente a la digitalización y cómo pueden impactar en los derechos de los consumidores?

Como he planteado en la ponencia, en el ámbito de los datos de salud —que afectan a la identificación de la persona en lo más profundo y de la que se derivan— yo creo que los sesgos y la discriminación son el principal problema, como ha señalado el director general de la Autoridad Nacional de Protección de Datos Personales.

Por razones de tiempo, no he podido incidir en las utilizaciones que están tajantemente prohibidas en el Reglamento del Espacio Europeo de Datos Sanitarios. Entre ellas se encuentra el artículo 35, que versa sobre el uso secundario de los datos para la toma de decisiones contractuales negativas o adversas para la persona. Los datos de salud no van a poder ser utilizados en tales casos. Lo más notorio y evidente es el ámbito de los seguros, pero este es también un tema relevante en otros entornos contractuales, como es el caso de los préstamos bancarios. La valoración sobre tu condición como buen o mal cliente depende de la salud que vayas a tener —las posibilidades de que no pierdas el empleo, de que no tengas bajas, etcétera—, afectan a la evaluación sobre el cumplimiento de devolución de un préstamo y, en definitiva, a la evaluación de tu solvencia futura.

* Directora de la cátedra y catedrática de Derecho Civil Foral de la Universidad Pública de Navarra, España. Vocal y profesora de la Scuola Dottorale Interateneo in Scienze Giuridiche Ca' Foscari, Venecia, Italia. Magistrada suplente en la Audiencia Provincial de Navarra, consejera del Consejo de Navarra, máximo órgano consultivo de la Comunidad Foral de Navarra y vocal del Consejo Asesor de Derecho Civil Foral de Navarra. Investigadora en múltiples proyectos en el ámbito español e internacional. Autora de más de un centenar de trabajos científicos sobre diversos temas de derecho civil. Miembro del consejo de redacción de diversas revistas.

** Integrantes del equipo de la revista *Ius et Praxis* y estudiantes de la Facultad de Derecho de la Universidad de Lima.

Otra de las restricciones de acceso para el uso secundario de los datos de salud que se fijan en el Reglamento del Espacio Europeo de Datos Sanitarios, tema apuntado en el Congreso, es la utilización de los datos de salud para el desarrollo de productos y servicios que pueden perjudicar a las personas y manipular a los consumidores. El propio artículo 35 del reglamento reseña, como ejemplo de aquello, el diseño de sustancias que puedan ser adictivas —drogas ilícitas, bebidas alcohólicas, productos del tabaco—; tenemos ya no solo sustancias químicas, sino también productos de videojuegos que generan situaciones adictivas. Por ejemplo, está comprobada la interrelación de quien resulta adicto a opiáceos con la existencia de problemas respecto a neurotransmisores y niveles de dopamina, a los que se intenta dar respuesta a través de sustancias químicas. Significa que, en muchas ocasiones, nuestras propias conductas dependen de nuestra propia configuración biológica, morfológica y biogenética. Resulta totalmente peligroso que todo esto esté en manos de quienes nos quieren vender una sociedad de consumo —como la que tenemos—, y de empresas que éticamente lo que quieren es la obtención de un beneficio a cualquier precio.

Por ello, la estructura del Espacio Europeo de Datos Sanitarios está diseñada para que exista un control en el uso y acceso a los datos sanitarios. Este se llevará a cabo mediante organismos designados por los Estados. Serán estos los que, valorando las finalidades para las que se solicita la utilización de estos datos, faculten su uso, lo controlen y lo supervisen.

El uso de datos personales para alimentar la inteligencia artificial (IA) genera debate. ¿Qué riesgos y beneficios plantea esta práctica para los consumidores, y cómo se podría regular sin frenar la innovación tecnológica?

Es una buenísima pregunta porque, precisamente, la gran cuestión que en estos momentos se plantea en Europa es cómo aprovechar tecnológicamente el avance de la IA para mejorar la oferta de productos y servicios —y, en definitiva, que el consumidor pueda acceder a buenos servicios a un precio muy razonable— sin que esto vaya en detrimento de la propia persona. Esta preocupación se plantea no solo en relación al derecho a la intimidad personal, sino también respecto de la propia consideración sobre el rol que la IA pueda tener en la sociedad.

En el ámbito de la salud, por ejemplo, se plantean las oportunidades que la IA ofrece para implementar la asistencia sanitaria a través de la telemedicina y de aplicaciones diagnósticas. En un entorno como el que tienen ustedes, con una geografía muy complicada, esta sería una solución para ofrecer una cobertura médica y asistencial en zonas remotas con eficiencia y un coste muy razonable. Casi todo el mundo cuenta con un terminal telefónico: diagnósticos perentorios o tratamientos que pueden resultar muy costosos podrían llegar a tiempo a través de esta vía; pero, también, la asistencia sanitaria directa se podría lograr a través de aplicaciones. En estos momento se están desarrollando diversas aplicaciones, las cuales se pueden encontrar en Google, que ayudan a los profesionales de la dermatología al

diagnóstico de enfermedades. Estas también prestan servicio directo al propio consumidor quien, al subir las fotos y datos de su afección, puede tener un diagnóstico de su enfermedad. Para que ello sea cada vez más fiable, se requiere alimentar a la IA con imágenes y datos de cómo se manifiestan determinadas enfermedades —erupciones, manchas, etcétera—, para así identificarlas y ofrecer un diagnóstico certero, con el consiguiente ahorro de desplazamiento o de atención. Esto va a suponer, sin duda, un gran avance para la medicina.

En el Perú, la telemedicina ha cobrado mayor relevancia desde la pandemia. Aunque contamos con una regulación marco, esta requiere ser actualizada y ajustada a la realidad del país, especialmente para abordar los desafíos que han surgido durante este periodo. La normativa de la Unión Europea, que muestra un desarrollo significativo en este ámbito y que incluye disposiciones avanzadas sobre protección de datos personales, se ha convertido en una referencia clave; es por ello que nuestro país la toma como modelo fundamental para fortalecer y mejorar nuestra legislación.

Está muy bien ver cuáles son las experiencias más avanzadas, pero sin olvidar cuál es la idiosincrasia y el entorno donde uno se mueve. Porque trasladar regulaciones sin ese punto crítico de cuál va a ser el entorno social y los medios que hay que implementar, puede terminar suponiendo que tengamos una legislación maravillosa, pero nada práctica ni aplicable.

Como experiencia y punto de reflexión, la normativa europea sobre protección de datos aplicados a ese ámbito resulta interesante. La Unión Europea no quiere perder la oportunidad, en la competencia que tenemos con el eje de Asia y el eje de Estados Unidos, de seguir estando a la cabeza en cuanto al uso de la IA, sin ceder en la defensa de la protección de datos, un derecho fundamental y estructural incorporado al Tratado de la Unión Europea y que es una salvaguarda para todos. Esta es una pieza fundamental para garantizar la dignidad de la persona, el libre desarrollo de la personalidad y, en definitiva, para hacer frente al avance que supone la tecnificación y lo que nos augura el futuro de una IA que puede terminar dominándonos. En ese punto, Europa se ha planteado como objetivo el establecimiento de varios espacios en los que se compartan datos para el aprendizaje profundo de los sistemas algorítmicos, a la vez que se fijan medidas que preservan los principios básicos para que la persona no pierda su condición y sus decisiones pasen a estar controladas por una máquina.

Entre los peores temores —los cuales compartimos— se encuentran las visiones que se plasman en las películas más apocalípticas, que nos muestran un futuro en el que las máquinas terminan dominándonos. Esto se vuelve aún más inquietante cuando lees declaraciones de ingenieros que admiten no comprender los mecanismos o las inferencias utilizadas por un sistema de *machine learning*. Por ejemplo, si una máquina cuenta con el sistema de *machine learning*, esta podría aprender todo un idioma a partir de una sola palabra. Este tipo de avances resulta realmente perturbador.

En este contexto, está claro que uno de los principales problemas es el de la trazabilidad: saber dónde se puede controlar y evitar que la máquina tome decisiones contrarias al ser humano. Muchas veces, el desafío radica en no saber de dónde proviene el conocimiento generado, aunque este pueda ser importante. De ahí también que me parezca fundamental que, si antes teníamos que estar todos muy bien formados, ahora esto sea más importante aún: ustedes, como estudiantes, no tienen que ahorrar tiempo y dedicación para pensar, estudiar y memorizar, ni deben dejar todo al albur de las máquinas, porque eso al final nos vuelve dóciles. Se necesita una formación profunda y crítica que nos permita saber y pensar con independencia del auxilio de la máquina.

Durante la pandemia del COVID-19, el uso de certificados de vacunación digitales planteó dilemas entre la privacidad y la salud pública. Desde su perspectiva, ¿cómo debió ponderarse el derecho a la privacidad de los consumidores con la necesidad de proteger la salud pública? ¿Qué opina sobre la obligatoriedad de presentar pruebas de vacunación y la divulgación de historiales médicos en este contexto?

Aquí estamos ante el gran debate que se ha extendido por todo el mundo, salvo en China, en donde, dado su sistema, todos los ciudadanos se sometían y no había ninguna posibilidad de discusión. Esto nos lo hemos planteado los países en los que los derechos fundamentales se protegen. Pero no hay que olvidar que los problemas de la pandemia no son de ahora, son históricos, y hay que adoptar decisiones razonables para evitar la propagación de las enfermedades.

En el Perú, en España y en el resto de países, las enfermedades infectocontagiosas se encuentran sometidas a un régimen jurídico especial de control y comunicación. Aquí, la ley, principio de legitimación, fija las medidas oportunas para que pueda conocerse cuál es el estado de los infectados y atajar los contagios. Todos sabemos que hay ciudadanos que son sensatos y respetuosos con el resto, y que, si han tenido un problema de salud, se han aislado; pero hay otros que no son tan responsables, que voluntaria o involuntariamente han propagado la enfermedad.

Como bien planteaba hoy la profesora Lourdes Zamudio, el derecho a la protección de datos no es un derecho incondicionado. Tiene límites y debe ser ponderado en su pugna con otros derechos, como el derecho a la vida, un ambiente socialmente protegido y la no producción de daños.

La gestión que se ha llevado a cabo me parece que se realizó como se pudo. Nos resultó sorprendente la situación. Nos habíamos olvidado de situaciones trágicas, como la peste que vivimos en Europa en el siglo xiv —1347 y 1352— o la epidemia de gripe de 1918. Se ha aprendido y, en ese aprendizaje, se han ido implementado mecanismos como, por ejemplo, las notificaciones a través de aplicaciones y el desarrollo de círculos de confianza. Estas herramientas permitían informar a las personas

de si se encontraban cerca de alguien que pudiera haber estado expuesto a la enfermedad, con el objetivo de promover entornos más seguros. No obstante, la situación se complicó, especialmente en lo relativo a los datos de salud, ya que, en algunos casos, la anonimización no resultó suficiente para cumplir con ciertos fines. La magnífica tesis doctoral del profesor Ronald Cárdenas va en esa línea del aprendizaje: las lecciones de la pandemia y los mecanismos para conseguir mejorar y aprender.

La siguiente pregunta se centra en el tratamiento que se da en el Perú cuando ocurre una vulneración de datos de salud. En nuestro país, cuando ocurre una filtración de información de salud, las clínicas tienen responsabilidad civil frente a los consumidores afectados por la filtración de su información. ¿Podría explicarnos cómo se aborda esta situación en el caso español y qué aspectos considera que podrían aplicarse al sistema peruano?

En el caso de España, dependiendo de si la sanidad es privada o pública, el régimen de responsabilidad es distinto. La mayor parte de los casos en los que ha habido una vulneración ha sido por accesos inconsentidos y, en el fondo, se trataba de actuaciones más bien reprochables, de cotilleo o búsqueda de información con fines espurios. De hecho, no conté [durante la ponencia] uno de los casos en los que se estableció una condena por revelación de secretos. Se trata de una sentencia de la Audiencia Provincial de Las Palmas en la que el ginecólogo, quien trataba a su propia esposa, se hallaba en un proceso de ruptura conyugal. Este había accedido a su historia clínica y había anotado que la esposa padecía algún tipo de enfermedad mental, aspecto que se desveló en el pleito de divorcio. Desde luego, esta es una situación extrema y merecedora de la sanción penal impuesta.

Cuando la vulneración se produce dentro del marco de la sanidad pública, opera la responsabilidad patrimonial de la Administración con la reparación del daño irrogado por el funcionamiento normal o anormal de esta. En teoría, el funcionamiento normal o anormal de los servicios públicos conlleva una responsabilidad de carácter objetivo. Pero, en la práctica, tratándose del ámbito sanitario, resulta insostenible un sistema objetivo. La jurisprudencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo de España, de manera constante, indica que la Administración no es una aseguradora universal, y que, en el ámbito de la salud, hay que ver si la responsabilidad se produce como una consecuencia de la infracción de la *lex artis ad hoc* del profesional sanitario, esto es, por no haber aplicado este el grado de diligencia exigible a su quehacer profesional.

En las ocasiones en las que se ha reconocido responsabilidad patrimonial por acceso a los datos de la historia clínica, puede advertirse tanto la culpa de quien accede como de parte de la organización, cuando esta última no adoptó las medidas técnicas adecuadas. En general, los centros sanitarios tienen preestablecidos protocolos técnicos de acceso a la historia clínica informatizada, para salvaguardar el derecho a

la intimidad del paciente, a la vez que para permitir el trabajo del profesional. Cuentan con sistemas en los que, aparte de dejar la huella de quien entra, queda justificado el porqué del acceso, denegándose este si se carece de autorización. Tratándose de centros privados, la vía para instar la reparación del daño por vulneración de la normativa de protección de datos se produce a través de la responsabilidad civil, y hay que acreditar cada uno de los elementos que hacen nacer esta.

Uno de los extremos que resulta especialmente complicado de probar es el de la producción del daño, ya que la mera infracción de la normativa de protección de datos y el mero acceso, por sí mismos, no entrañan un daño. Se necesita acreditar que ha existido un daño. El daño que generalmente se suele invocar es el daño inmaterial, que se concreta en un daño moral. El problema del daño moral es que técnicamente su prueba siempre ha sido muy compleja. De ahí la importancia de la sentencia del Tribunal de Justicia de la Unión Europea del 11 de abril del 2024, relativa a la consideración de que el temor a que determinados datos personales sean conocidos por terceros, siempre que acredites que tienes ese temor, puedes fundamentar un daño moral. De ahí la utilización e invocación que se ha venido efectuando, en España, de la Ley 1/1982 de "Protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen", cuyo artículo 93 ha permitido que, acreditada la situación de una infracción tipificada en la ley, automáticamente se valore la existencia de un daño moral.

En el marco de su ponencia, ¿qué acciones considera esenciales para que las instituciones de salud cumplan con su responsabilidad en la protección de datos de los pacientes y para que fortalezcan la confianza de los consumidores en sus servicios, a efectos de evitar problemas de responsabilidad civil?

Yo creo que todas las instituciones sanitarias, tanto en Europa como aquí, tienen muy interiorizada la necesidad del cumplimiento de la normativa de protección de datos, entre otras cosas porque el incumplimiento de esa normativa por parte del profesional puede conllevar pena de cárcel. El delito de revelación de secretos o de confiabilidad es uno de los mayores garantes, junto con las políticas que desarrolla la Autoridad Nacional de Protección de Datos Personales del Perú. La autoridad —ya lo ha comentado hoy el director general— depende del Ministerio de Justicia.

Una de las exigencias en Europa es que la autoridad sea un organismo independiente, que pueda actuar de una forma objetiva, viendo cuáles son las necesidades, y con una actividad pedagógica y didáctica constante de educación a los colectivos. Los cursos de sensibilización sobre la materia son fundamentales, así como las campañas que incentivan a los responsables del tratamiento de datos y a los delegados de protección de datos a redoblar esfuerzos para garantizar el cumplimiento normativo y evitar posibles sanciones.

En esta misma línea, como consumidores de servicios digitales, ¿qué medidas prácticas recomendaría a los ciudadanos para proteger sus datos personales, particularmente los datos de salud, frente a posibles vulneraciones?

Pues, no darlos; tan sencillo como ser muy celoso de la información que quieres compartir, solo compartirla cuando sea estrictamente necesario y ser consciente de la importancia del dato que ofreces. Por ejemplo, si ustedes van a contratar un arrendamiento para vivir, el arrendador no tiene por qué saber cuál es su estado de salud. Solemos encontrarnos con unas contrataciones en las que, sin querer, la petición de datos es indebida. El principio de licitud en el tratamiento de los datos y de la proporcionalidad en el acceso a estos vienen dados por la cuestión de para qué quiere usted los datos. Hay que ser exigentes y reivindicativos en este punto.

Entendemos, entonces, que esto está directamente relacionado con la necesidad de sensibilizar a la población sobre la importancia de proteger sus datos personales. Recuerdo haber leído una noticia en España sobre una gran filtración de datos en el Banco Santander debido a un ataque de *hackers*. Una situación similar ocurrió en el Perú con el banco Interbank, en el que se produjo el *hackeo* de datos de gran parte de sus clientes. Al consultar a las personas afectadas, muchas comentaron que no se preocupan porque no habían sufrido robos en sus cuentas bancarias. Sin embargo, no son completamente conscientes de que, ahora, terceros pueden acceder a información sensible, como su domicilio o su actividad financiera. Esta situación resaltaría la urgente necesidad de que nuestras autoridades implementen acciones que promuevan la concienciación y la información sobre la protección de estos datos.

Claro. Sin embargo, los recursos de la autoridad son limitados y no pueden llegar a todo. Otro ejemplo de la falta de conciencia con respecto a compartir nuestros datos es cuando queremos acceder a determinadas páginas. Muchas de ellas te dan la opción de "acepto todo" o "deniego todo", y, a veces, la persona no lee qué es lo que acepta o no acepta. Si uno va rápido y necesita una determinada información, decidimos que sí, puesto que no tenemos paciencia. Con eso juegan también.

Todo lo que se ofrece gratis en internet tiene un precio: el precio eres tú. En este contexto, la Directiva (UE) 2019/770 sobre contratos de suministro de contenidos y servicios digitales, que fue incorporada al artículo 59 de la Ley General para la Defensa de los Consumidores y Usuarios en España, contempla la posibilidad de obtener bienes y servicios digitales a cambio de datos personales.

El Supervisor Europeo de Protección de Datos cuestionó la inicial redacción de la norma y que pudiera existir "pago" de bienes y servicios a cambio de datos personales, modelo de negocio que nos viene del ámbito anglosajón. Desde el punto de vista teórico, esto ha planteado el tema de la calificación del dato personal como un bien patrimonial o extrapatrimonial, pues todos los derechos fundamentales están sujetos a un régimen

extracomercial para poder tener control sobre los mismos. Por ejemplo, si obtienes un bien o servicio a cambio de proporcionar tus datos personales, esto podría entenderse como una contraprestación similar al pago en un contrato de compraventa. Si, en este contexto, decides no proporcionar los datos o retirar tu consentimiento después de haberlo dado, una vez que ya has recibido el bien o servicio, se generaría una situación comparable al incumplimiento de una de las partes en un contrato de compraventa.

En ese caso, ¿sería posible ejercer mis derechos? Por ejemplo, en el contexto de un contrato de compraventa, si decido no proporcionar mis datos o, habiendo ya recibido el bien o servicio, si quiero revocar mi consentimiento, pero la otra parte alega incumplimiento, ¿podría defender mi derecho a revocar el consentimiento argumentando que se trata de un derecho fundamental?

En teoría, sí; y eso es lo que se ha planteado en un sector de la doctrina. Sin embargo, si se revoca el consentimiento una vez que se ha obtenido el bien o servicio, podría generarse un enriquecimiento injustificado por parte del consumidor, lo que obligaría a resarcir a la otra parte. De hecho, respecto al negocio de los datos, resulta que los datos que más se pagan en la *deep web* son los datos de salud. En el fondo, el asunto de los datos genera los debates clásicos. Si hay un desplazamiento patrimonial o un beneficio a favor de una de las partes, si se pierde la causa de atribución, hay que reequilibrar la relación. Esta es una de las tantas situaciones o ejemplos del problema que generan los datos.

En el Perú, los datos de salud son clasificados como datos sensibles, lo que implica una regulación más estricta. Un ejemplo de ello es la Directiva Administrativa 294-MINSA/2020/OGTI, emitida por el Ministerio de Salud, la cual regula específicamente el tratamiento de este tipo de datos. Además, existe la norma técnica de historia clínica, que también aborda el manejo de estos datos dentro del marco normativo vigente. Al día de hoy pareciera que, al menos en este sector, estamos realizando mayores esfuerzos para continuar protegiendo los datos, garantizando que, por un lado, las empresas lleven a cabo su labor de manera eficiente y, por otro, que los consumidores se sientan seguros y satisfechos con el tratamiento de su información.

Desde luego, los centros de salud son muy conscientes de la importancia de tutelar adecuadamente estos datos. El problema es que, en unos determinados casos, las brechas de seguridad existen. Por mucho que se pretenda o intente poner "puertas", hay ocasiones en las que ello no resulta suficiente.

En España, ¿qué infracciones enfrentan las empresas que no tutelan adecuadamente los datos de sus usuarios?

En España, el Reglamento General de Protección de Datos, el cual se aplica en toda la Unión Europea, establece un régimen sancionador basado en la valoración del incumplimiento. El sistema actual —a diferencia de lo que hemos tenido hasta fechas recientes— exige

que el responsable de la protección de datos diseñe un plan que contemple todas las circunstancias posibles que podrían surgir, tanto las comunes como las excepcionales. Esto implica una obligación general de protección de los datos, con responsabilidades tanto en los medios como en los resultados. Dependiendo del grado de negligencia en el cumplimiento de estas obligaciones, las infracciones y sanciones se fijan dentro de un rango amplio y se adaptan a la gravedad del incumplimiento.

Finalmente, ¿qué puede aprender el Perú de la experiencia de España y la Unión Europea en la protección de datos personales en sectores sensibles como la salud, desde la perspectiva de los derechos del consumidor?

Creo que, en el Perú, ya se está reflexionando sobre este tema. Las autoridades peruanas, como el director general [de la Autoridad Nacional de Protección de Datos Personales], el profesor Eduardo Luna, y la profesora Zamudio, mantienen un contacto constante con las autoridades encargadas de la protección de datos tanto de Iberoamérica como de Europa, lo que les permite intercambiar experiencias.

Hay que ir, primero, consolidando progresivamente la cultura en materia de protección de datos. Hay que dotar de medios al sistema de protección de datos y, en función de las experiencias que se van teniendo, adoptar decisiones que permitan ir avanzando, en el ámbito de la salud, hacia el mejor tratamiento de los datos por parte de los centros sanitarios, con las medidas y guías que puedan servir de ayuda. En ese mismo ámbito, en algún determinado momento, yo supongo que el hermanamiento de todos los países que integran esta parte tan preciosa del mundo implicará un movimiento transfronterizo —que ya existe— con la necesidad de la creación de un espacio de comunicación de datos. Ahí, la experiencia que pueda tener Europa puede resultar interesante en esa puesta en común de los datos para finalidades que, en el ámbito de la salud, son fundamentales para los investigadores y las profesionales que se dedican a la medicina.

El tema de la medicina personalizada parte de la obtención de una información no sesgada que permita conseguir que en el *machine learning* se produzca un aprendizaje profundo, y que, por ejemplo, según las características de una determinada persona, identifique la dispensación de la medicación que le sea necesaria. Este enfoque se complementa con otros elementos, como los *waivers*, aplicaciones que ajustan la medicación o el tratamiento según las necesidades de cada momento. Además, se considera la singularidad de ciertas enfermedades. Hoy, por ejemplo, bajo el término de cáncer hay una multiplicidad de situaciones en las que apreciamos un crecimiento masivo de células, pero no sabemos muy bien a qué responden; o bien, tenemos a las enfermedades neurodegenerativas: detrás de lo que se denomina Parkinson hay múltiples realidades. Así, una medicina personalizada y un aprendizaje de cada una de estas características permite que el tratamiento —incluso la anticipación a la problemática que uno pueda tener, por sus características genéticas en el momento en que se desenvuelvan— adelante la solución y nos ayude, en teoría, a vivir mejor.

En el ámbito de la investigación parece fundamental la utilización de los datos de salud para seguir avanzando. De hecho, la normativa española, la "Ley orgánica de protección de datos personales y garantía de los derechos digitales", en una de sus disposiciones adicionales (la decimoséptima), contempla la posibilidad de que —siempre que estén anonimizados o con posibilidades de pseudoanonimización— los consentimientos respecto de ese tratamiento permitan también utilizar esos datos para la investigación. Este es un planteamiento que, como experiencia, puede resultarles interesante.

Actualmente, estoy trabajando en un proyecto sobre los organismos de gestión altruista de datos en el ámbito sanitario. Estos entes, como fundaciones o asociaciones, recibirían los datos a través de una donación voluntaria por parte de los titulares de los mismos, que pueden ser tanto personas físicas como administraciones. ¿Con qué objetivo? El propósito es facilitar estos datos para los fines que ya hemos mencionado: mejorar la gestión en la atención y la previsión por parte de la Administración.

El proyecto que comenta podría ser de gran ayuda, especialmente para sectores sensibles, como el ámbito del cáncer, el cual plantea desafíos legales y éticos importantes.

Uno de los puntos importantes a considerar es la colaboración del sector médico con el jurídico y que las previsiones legales en materia de protección de datos no se vean como limitaciones. En este ámbito, se plantea un reto semejante al que se suscitó en la contratación electrónica con los profesionales de la ingeniería. La legislación no es una restricción, sino una salvaguarda de los derechos. Por ello, hay que pensar en un marco legal adecuado para proteger tanto los datos de los pacientes como los avances en la medicina.