redacción médica

Opinión

Claves del proyecto Nightingale de Google

RICARDO DE LORENZO, PRESIDENTE DEL BUFETE DE LORENZO ABOGADOS
DOM 24 NOVIEMBRE DE 2019. 20.30H
POR LEY

La semana pasada el diario **'The Wall Street Journal'**, denunciaba como consecuencia de una investigación propia, **como Google**, había accedido a los datos médicos personales de millones de pacientes residentes en 21 de los 50 estados de **EEUU**, todos ellos de la compañía hospitalaria Ascensión, el segundo sistema de salud más grande de Estados Unidos y que tiene su sede en San Luis (Misuri), con cientos de clínicas y hospitales en esos estados, a los que podrían tener acceso los empleados de Google, que participan formalmente en el proyecto, bautizado como **'Project Nightingale'** (Proyecto Ruiseñor).

Según el diario neoyorquino, el gigante de **Silicon Valley**, habría compilado, junto a los nombres de estos pacientes, fechas de nacimiento, etnia, historial médico y tratamientos recibidos, junto a los resultados de análisis, diagnósticos médicos y registros hospitalarios. Ni los pacientes, ni los doctores de la red hospitalaria estaban al corriente del trasvase de información, según esta publicación, lo que, al conocerse, motivó que Google y el grupo sanitario Ascensión **firmaran formalmente el acuerdo de transferencia de datos pocas horas después de que se publicará esta información.**

Acuerdo tras el que se ha remitido un comunicado, a **'The Wall Street Journal'**, en el que Google defiende que su proyecto cumple con las leyes federales sobre protección de datos médicos, siendo su objetivo **"en última instancia, mejorar los resultados, reducir los costos y salvar vidas"**, señaló el presidente de Google Cloud, **Tariq Shaukat**, en la citada nota de prensa sobre el acuerdo alcanzado con Ascensión.

Según se informa, ambas compañías están probando un software para que los Médicos puedan buscar información de los pacientes por categorías y de forma analítica y organizada, con el objetivo de dar a los profesionales sanitarios un mejor acceso a los datos del paciente, mejorar su atención y, a la larga, **utilizar esos datos para diseñar un tratamiento más efectivo.**

Según el acuerdo hecho público, los datos se almacenan en un espacio privado de la nube -sistema de almacenamiento de información 'online'- de **Google.** Defendiendo ambas compañías la legalidad de que las entidades médicas puedan compartir los datos de pacientes con compañías dedicadas a la gestión informática de los mismos. Al mismo tiempo, ambas compañías niegan que suponga un uso inadecuado de la información personal de los pacientes, **así como el software utilizado por Google para procesar la información que entienden respeta la legislación de protección de datos médicos estadounidense** (HIPAA, en sus siglas en inglés).

Llegados aquí, la pregunta obligada sería, si esto mismo es posible en nuestro país, y para ello es necesario analizar la legislación sobre protección de datos americana frente a la europea y específicamente la española.

En Estados Unidos no existe una legislación federal que proteja los datos de los usuarios y la privacidad equiparable a nuestro Reglamento General de Protección de Datos (RGPD), reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos que ha sido de aplicación en nuestro país desde el pasado 25 de mayo de 2018, o a nuestra Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, de 6 de diciembre de 2018 acorde con el RGPD, sino más bien al contrario. **Solo existen normativas sectoriales que regulan diferentes ámbitos como, por ejemplo, la Ley de Protección de la Privacidad de Menores de los Estados Unidos** (Coppa), la Ley de Cumplimiento Fiscal de Cuentas en el Extranjero (FATCA) y específicamente en el ámbito salud, que estamos tratando, la Ley de Transferencia y Responsabilidad del Seguro Médico en EEUU.

(Health Insurance Portability and Accountbaility Act o HIPAA), que es la que regula el tratamiento de los datos de salud, permitiendo a los hospitales ceder los datos de sus pacientes a terceros sin informar a los mismos.

La diferencia clave entre el Reglamento General de Protección de Datos (RGPD), y la Ley de Transferencia y Responsabilidad del Seguro Médico (HIPAA), se basa en el enfoque. EL RGPD se centra en el ciudadano de la UE, cualquier organización establecida en la UE que trate datos de ciudadanos europeos está sujeta a esta normativa, independientemente de donde se estén tratando los datos. En oposición, l**a HIPAA es de aplicación a toda organización que transmita electrónicamente o almacene información de salud dentro de los Estados Unidos, de esta forma el Gobierno norteamericano prefiere colaborar con estos gigantes tecnológicos para poder recabar información y vigilar masivamente a empresas y ciudadanos.**

¿Qué sucede en Europa?

Y en cambio Europa intenta regular a través de sus leyes el comportamiento de las grandes multinacionales, garantizando a través de Autoridades de Control, la privacidad y la protección de datos de sus ciudadanos. Un claro ejemplo es la Declaración común del Grupo de Contacto de las Autoridades de Protección de Datos de Holanda, Francia, España, Hamburgo y Bélgica contra Facebook, tras el anuncio de Facebook, el 13 de noviembre de 2014, de revisar globalmente su política de privacidad, su política de cookies y sus términos de uso, que ha permitido a estos países iniciar investigaciones nacionales relacionadas, entre otros aspectos, con la calidad de la información facilitada a los usuarios, **la validez del consentimiento y el tratamiento de datos personales con fines publicitarios.**

Además, el Gobierno norteamericano no dispone de ninguna autoridad u organismo que vele por la privacidad y la protección de datos de los ciudadanos y si, finalmente, algún conflicto sobre esta temática llega a juzgados, las sanciones impuestas se deciden caso por caso, sin tener estipulado de antemano la gravedad de las acciones.

En consecuencia, a través del Proyecto Nightingale, Google está recopilando los datos de salud de los pacientes con la finalidad de crear una especie de **“Google sanitario”** que funciona de la siguiente manera: A). El paciente ingresa al hospital, al consultorio del médico o al centro de atención para personas mayores. B). Los médicos o personal sanitario con competencia examinan al paciente e ingresan los datos en el sistema informático que se almacenan instantáneamente al sistema **"Project Nightingale" de Google.** Y C). El sistema puede sugerir los siguientes resultados, entre otros: i.- Planes de tratamiento, realización de pruebas, desviaciones inusuales

en la atención. ii.- Reemplazar o añadir médicos al tratamiento del paciente y iii.- Aplicación adicional de pruebas de detección de estupefacientes.

El proyecto pretende combinar varias tecnologías disruptivas, tales como el big data, inteligencia artificial y machine learning con el fin de mejorar la asistencia sanitaria. **El software creado utilizaría los datos del paciente introducidos por el médico para asesorarle en lo relativo al tratamiento** y en las decisiones a tomar. Describiendo Google el proyecto como una "capa" de información del paciente que, en definitiva, conforma la historia clínica del mismo. Esta historia clínica sería accesible por parte del personal médico de manera remota, de modo que facilita la interoperabilidad de datos de salud entre diferentes centros sanitarios. No obstante, también tienen acceso a esos datos los empleados de Google, de ningún modo relacionados con la asistencia sanitaria. Ello podría llevar al incumplimiento de la HIPAA puesto que ese acceso por parte de los empleados de Google sobrepasará la finalidad estricta de **atención médica.**

Además, la plataforma, tal y como la han presentado los creadores, no cuenta con ninguna restriccion de accesos. Si se empieza a escribir un nombre, Google automáticamente produce un menú desplegable con otros pacientes con nombres similares. De modo que se puede llegar a tener acceso a un número ilimitado de datos sin ningún tipo de control. **Esto contradice claramente el principio de minimización de datos consagrado en la normativa Europea y específicamente en España.**

Nuestro reglamento califica como categorías especiales de datos personales aquellas que «revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física» considerando los datos de salud como especialmente protegidos y **prohíbe expresamente su tratamiento excepto en supuestos tasados, entre otros, cuando sea necesario para la prestación de asistencia sanitaria.**

En este mismo mes la **Agencia Española de Protección de Datos**, ha sacado la Guía para pacientes y usuarios de la Sanidad, tratando los datos relativos a la salud junto a los datos genéticos, como datos personales relativos a las características genéticas heredadas o

adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Por tanto, los datos personales existentes en bases de datos sanitarias son de dos tipos: los que identifican a la persona, tales como nombre y apellidos, dirección, teléfono, DNI, número de tarjeta sanitaria, etc…; y toda la información acerca de su estado de salud, tales como pruebas diagnósticas, cirugías, medicamentos, antecedentes familiares, etc., información que se configura en la Historia clínica, que regula 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.**

Secreto profesional

En esta Guía se establece específicamente que no es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de datos personales y de salud si se van a utilizar para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o **gestión de los sistemas y servicios de asistencia sanitaria y social.** (La base de legitimación para este tratamiento de datos está establecida en el artículo 6.1.b) del RGPD para las entidades aseguradoras de salud privadas, y en el artículo 6.1.c) del mismo Reglamento para la sanidad pública).

También se pueden tratar los datos de salud sin solicitar el consentimiento cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, o cuando lo solicite un órgano judicial. (La base de legitimación está establecida en el artículo 6.1.d) del RGPD).

Las personas que traten los datos deben ser profesionales sujetos a la obligación de secreto profesional, o que estén bajo su responsabilidad, (principio de vinculación).

La guía de la Agencia contempla entre otros principios en el tratamiento de los datos los de la limitación de la finalidad: es decir que deben recogerse con fines determinados, explícitos y legítimos, y no serán usados posteriormente para finalidades incompatibles con

dichos fines.

Otro sería el de minimización de datos: es decir que sólo se van a utilizar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; es decir, que solo van a recoger, en general, los datos mínimos necesarios para prestar la mejor asistencia sanitaria. Y por último el de integridad y confidencialidad: **los datos personales sólo podrán ser tratados de tal manera que se garantice una seguridad adecuada de dichos datos**, incluida la protección contra el tratamiento y acceso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

En consecuencia, **esta información debe ser anonimizada si quiere cumplir con la normativa europea y seguir protegiendo la privacidad sanitaria de los usuarios.**