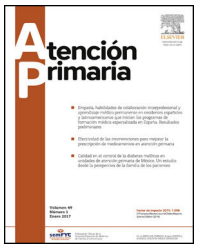
Aten Primaria. 2020;52(8):521–522

Atención Primaria

www.elsevier.es/ap



EDITORIAL

Implicaciones para el personal sanitario de la entrada en vigor del Reglamento (UE) de Protección de Datos de la Unión Europea

Implications for healthcare personnel of the entry into force of the european union data protection regulation

La entrada en vigor del Reglamento (UE) de Protección de Datos ha supuesto un importante hito en la acelerada historia de Internet, los *big data* y la inteligencia artificial. Esta normativa trata de afrontar, al menos en el territorio de la Unión Europea (UE), uno de los mayores retos de la historia de la humanidad: el tratamiento de la información que generamos los seres humanos, lo que afecta a esferas tan íntimas como la ideología, la genética, la personalidad, la adscripción étnica, etc. La forma en que suministramos esta información puede ser consciente o inconsciente, voluntaria o involuntaria pero, sin duda, resulta sumamente valiosa tanto para el sistema económico como para quienes monopolizan el poder.

El personal sanitario, en sentido amplio, se ha situado en la primera trinchera de este nuevo escenario, donde ha de compatibilizar el secreto médico con la necesidad de recabar, almacenar y compartir información para realizar su trabajo con eficacia; su buena fe, con un contexto jurídico cada vez más mercantilizado, y su juramento hipocrático, con la ingenuidad del ciudadano medio que abraza con fervor cualquier aplicación informática donde figure la leyenda de la gratuidad.

Pues bien, la entrada en vigor de la normativa que citamos está generando dudas acerca del alcance de expresiones como «bases de datos», «autorización», «almacenamiento», etc. Por ejemplo, el listado de los alumnos que tutorizamos en prácticas en nuestro hospital, ¿es una base de datos a efectos legales? ¿Debemos contar con su consentimiento individualizado, dar de alta en la Agencia de Protección de Datos, informarles de cómo pueden darse de baja o rectificar sus datos, etc.? Dado que todavía hay mucho terreno por concretar, lo mejor es adoptar una política defensiva, esto es, no arriesgar y tomar las precauciones necesarias para evitar reclamaciones o responsabilidad civil. Por ello, ante la duda, es mejor considerar «dato» cualquier información que manejemos como consecuencia del ejercicio de la profesión, y actuar en consecuencia.

Los sistemas de comunicación entre el personal sanitario deben ser objeto de una especial precaución. Los programas informáticos que permiten la comunicación instantánea (aplicaciones para el teléfono móvil, correos electrónicos, etc.), no son gratuitos, ni muchísimo menos. El precio somos nosotros, que nos convertimos en sujetos pasivos para la publicidad, pero, sobre todo, en agentes activos que suministramos información personal a los titulares de dichos programas, que a su vez lo empaquetan y venden a terceros. Y si esto puede ser un verdadero problema en nuestra vida privada (v. gr., cedemos a perpetuidad las fotos de nuestros hijos), en el caso clínico puede constituir un verdadero drama.

Por ese motivo, no se deben compartir historiales clínicos, fotos, comentarios, análisis, imágenes, etc., a través de estas aplicaciones, ni siquiera entre profesionales de la sanidad, ya que se está suministrando una copia al titular de dicha aplicación (reitero: al hacer uso de la aplicación, firmamos un contrato legal de cesión. La ilegalidad la cometemos nosotros, al compartir información médica a través de dichas aplicaciones). Estos datos que de forma inocente se intercambian a través de esos servicios, a veces buscando una finalidad legítima (v. gr. consultar con otros especialistas), pueden ser objeto de almacenamiento, comercialización y distribución, con efectos colaterales que mostrarán su verdadera dimensión en los próximos años.

Incluso en caso de reclamación judicial contra el personal sanitario (responsabilidad civil o penal), el almacenamiento de esta información puede ser un problema *a posteriori*, ya que muchas veces se pierde el contexto en que fue formulada, los objetivos que se tenían en mente al ser elaborada,

https://doi.org/10.1016/j.aprim.2020.01.003

o la información está fragmentada, lo que puede poner en peligro la seguridad jurídica de médicos y enfermeros. Hemos de tomar conciencia de que vivimos en una especie de *Gran Hermano* a escala mundial, donde la información que suministramos se recoge en soportes que permiten su «resurrección» en una época, contexto o situación completamente inesperada para quien la suministró.

Por otra parte, el reglamento europeo se ha elaborado con la finalidad de imponer obligaciones a los gigantes informáticos, cuya sede reside en EE. UU.. La globalización ha producido un efecto paradójico, y es que en territorio europeo prestan servicios empresas cuya sede está en otros lugares (la legislación aplicable la marca el domicilio donde están registradas las empresas). Si nos resulta difícil imaginar entablar un pleito contra un gigante informático en EE. UU. (v. gr., para borrar el perfil genético de un paciente), pruebe a imaginar el pleito en territorio chino. Por ese motivo, aunque resulta loable el intento europeo de someter a control el salvaje oeste informático, en muchos aspectos resulta completamente insuficiente. Basta recordar la dificultad que supone que las multinacionales informáticas paguen sus impuestos en territorio UE. En resumen, y a pesar del rigor y amplitud del reglamento europeo, lo mejor, desde el punto de vista individual, máxime si se es profesional sanitario, es prevenir; y la mejor técnica es evitar compartir información médica sensible si no se tiene la absoluta certeza de que el medio para recabar y compartir información es seguro.

Por este motivo, con total independencia de si se trabaja para un centro hospitalario, ambulatorio, consulta, etc., y de que este sea público o privado, la empresa titular debería suministrar al personal sanitario sistemas de comunicación informáticos que cumplan escrupulosamente con el Reglamento de Protección de Datos. Lo deseable es que no solo afecte a los sistemas informáticos (v. gr., servidores propios o empresas externas sujetas a la legislación europea), sino también a las aplicaciones para los teléfonos móviles (el riesgo no es comunicarse oralmente, dado que solo se puede grabar la conversación por mandato judicial, sino escribir o intercambiar archivos, que quedan almacenados en servidores fuera de nuestro control). Es decir, todo sistema de recolección de datos, intercambio de información, comunicación, etc., debe estar bajo el control de la empresa, pública o privada, lo que proporcionaría seguridad jurídica al personal sanitario. También es razonable no comunicarse con los pacientes a no ser por estos medios seguros. Hemos de tener en cuenta que no sabemos qué nos deparará el futuro. Las muestras de sangre, tejido, etc., que hasta hace poco eran anónimas, ahora pueden ser reidentificadas mediante las modernas técnicas de análisis de ADN proporcionadas por los *big data*. Es decir, las personas que en el pasado proporcionaron muestras creyendo que iban a ser siempre anónimas, pueden contemplar hoy con estupor cómo las compañías de seguros o las empresas de contratación laboral han conseguido su perfil genético. Las consecuencias pueden ser devastadoras. Por ese motivo, en el tratamiento de los datos sensibles desde el punto de vista sanitario no solo se debe tener en cuenta el principio de autonomía (v. gr., pedir autorización al titular de los datos), sino también el de precaución, esto es, tomar medidas frente a riesgos que ni siquiera hoy podemos prever (riesgo al cuadrado, desconocemos lo que desconocemos).

Manuel Jesús López Baroni
Universidad Pablo de Olavide, Sevilla, España