Asociación de Internautas

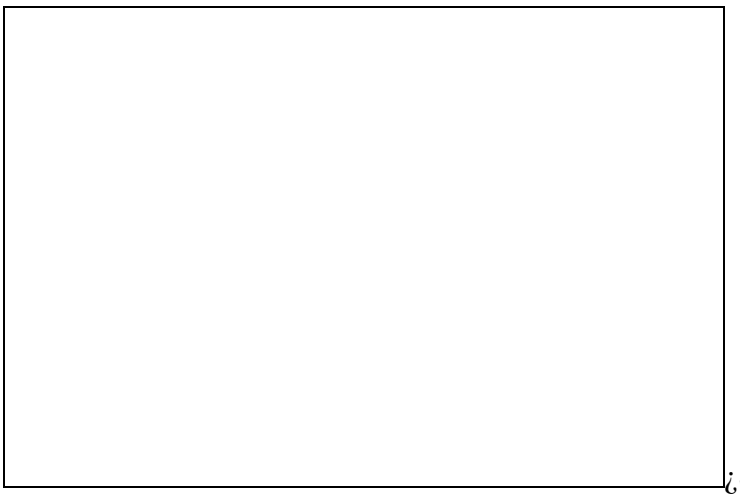
¿Somos anónimos en el mundo open data?

La protección de los datos personales cada vez se sitúa como una de las principales preocupaciones de los usuarios en Internet. Bien es cierto que la sociedad actual vive esa bipolaridad entre el celo por la privacidad y la barra libre de información personal que se vierte en las redes sociales como Facebook o Instagram.

Sin embargo, la verdad es que la privacidad importa, como demuestran los datos que ha facilitado hoy el director de la **Agencia Española de Protección de Datos (AEPD)**, José Luis Rodríguez Álvarez, durante la celebración en Madrid de su 7ª Sesión Anual Abierta. Tal y como ha expuesto el director, **tras la sentencia favorable al derecho al olvido en Internet,** ya no es sólo que en el último año **la Sala de lo Contencioso-Administrativo de la Audiencia Nacional haya desestimado 54 de los 72 recursos que interpuso Google** (más otros cuatro desestimados parcialmente), sino que el propio motor de búsqueda ha optado por desistir nada menos que 136 recursos.

En este contexto de datos y riqueza de información, aparece una nueva derivada que puede complicar el asunto: los denominados *open data*, es decir, esa ingente cantidad de información pública cuya reutilización se está fomentando desde organismos como la propia Unión Europa con directivas como la 2013/37/UE. Al respecto, Rodríguez Álvarez está convencido que **el auge de los *open data ?beneficiará el desarrollo de la Sociedad de la Información y del crecimiento económico?*** pero, al mismo tiempo, advierte de que ***?pueden crecer los riesgos para la protección de datos personales si no se toman las medidas oportunas?***.

La propia AEPD está ya elaborando una guía sobre los datos personales en este contexto de reutilización para simplificar el seguimiento de unas directrices que garanticen la protección de los datos personales. Una guía, además, que aspira a ser lo más consensuada posible y que, *?cuando esté redactada, se someterá a debate público para enriquecerla antes de concluir la versión definitiva?*, indica el director de la AEPD.



¿Significa esto que el extraordinario potencial que traen consigo los *open data* podría irse al traste por no ser compatible con la LOPD? En realidad no, hasta el punto de que es posible conseguir que ni siquiera se les aplique esta ley de protección de datos personales. Eso sí, según establece la Directiva 2013/37/UE, además del respeto

por los datos personales, éstos no deben ser reutilizados de un modo incompatible con las finalidades para los que fueron recogidos.

Una de las claves para minimizar al máximo los riesgos de vulneración de los datos personales en esta reutilización de la información pasa por la anonimización de ésta. Tal y como explica María José Blanco, secretaria general de la AEPD, la anonimización supone conseguir la *?ruptura de la cadena identificación-información, buscando que ésta sea irreversible o que para revertirla se requiera tanto esfuerzo que no merezca la pena?*. Esa eliminación de datos identificadores sería la que le eximiría de la aplicación de la LOPD.

Un proceso, por otro lado, que no resulta tan sencillo como pudiera parecer en un principio y que va más allá de la preanonimización, que incluiría el inventario de las variables de información, la eliminación de identificadores y de la otras variables o, al menos, su reducción. Tras ese paso y mediante técnicas de encriptación, aleatorización o generalización, entre otras, sería cuando se procedería a la anonimización en sí misma, que puede reforzarse con otras herramientas complementarias y refuerzo de las medidas de seguridad (la pseudoanonimización).

El peligro de la reidentificación

Dados los últimos avances en computación y procesamiento masivo de datos, lo que comúnmente se conoce como *big data,* ya no basta con anonimizar un dato específico y pensar que con eso será imposible revertir el proceso. Hoy en día y con la cantidad de información disponible en la red, incluso si también ésta se encuentra anonimizada, **se podrían cruzar diversas fuentes de datos (blogs, redes sociales, buscadores, medios de comunicación, fuentes abiertas, geolocalización?) y proceder a una reidentificación de un individuo.**

La Opinión 5/2014 sobre técnicas de anonimización, elaborada por el Grupo de Trabajo del artículo 29 de la Comisión Europea, destaca algunas de estas técnicas de reidentificación, entre las que sobresalen el ?*singling out?,* con la que es posible identificar a un individuo en un repositorio de información a partir de un dato específico como su código postal o se fecha de nacimiento; el *?linkability?* o, es decir, el cruzado de datos procedentes de diferentes fuentes de información; y el *?inference?*, por la que através de la información que rodea a un individuo es posible deducir con bastante acierto un dato específico de su identidad, como es su ciudad de residencia si todos sus contactos próximos tienen una ubicación concreta en común.

Por este motivo, cuando se arranca un proceso de reutilización de información y se opta por la alternativa de la anonimización, es preciso tener en consideración toda una serie de factores, entre los que Blanco subraya qué otros datos están disponibles para el público o para los reutilizadores y qué probabilidad real existe de proceder a la reidentificación, ya sea persiguiendo fines comerciales, coercitivos (recobro), uso de información de personajes públicos o, incluso, fines malintencionados como el acoso o la intimidación.

?Se trata de un proceso vivo, que en absoluto es estático?, explica Blanco, *?es muy dinámico dada la cantidad de actores que entran en juego, por lo que el riesgo de reidentificación puede variar a lo largo del tiempo?*; es decir, que **lo que hoy parece que goza de una anonimización irreversible puede mañana dejar de hacerlo si no se han tomado las debidas precauciones.**

En este sentido, según explica la secretaria general de la AEPD, es importante que quien procesa a la anonimización de la información sea el organismo que autoriza la reutilización, que a fin de cuentas es quien mejor conoce el dato. Este organismo es, además, no sólo quien mejor puede

evaluar los riesgos de reidentificación, sino también quien puede aplicar procedimientos de anonimización desconocidos para el reutilizador.

A pesar de todas estas medidas de precaución y dado que la anonimización totalmente irreversible para siempre parece muy complicada de conseguir, Jesús Rubí, adjunto al director de la AEPD, explica que se han puesto en marcha una serie de garantías jurídicas como es la prohibición de reidentificar, así como de utilizar datos personales para la adopción de decisiones sobre los afectados. En esta misma línea, entre esas garantías jurídicas también destaca el ofrecimiento a los interesados de medios para alertar sobre la reidentificación y, por supuesto, la imposición de medidas coercitivas (suspender o poner fin a la accesibilidad a los datos, sanciones económicas?) a quien viole esa protección de los datos personales.

Reproducido de SinDominio.es
