FIRMA INVITADA

Efrén Díaz Díaz

Protección de datos: lecciones del caso Facebook

Además de cumplir con la regulación vigente sobre protección de datos, convendría que las redes sociales asumieran que la privacidad está por encima de intereses comerciales o electorales.

¿QUÉ DATOS PUEDEN SOLICITAR las redes sociales a sus usuarios? Hay que reconocer que, legalmente, muchos. ¿Y dónde puede terminar esa información? La respuesta no resulta evidente en absoluto, especialmente a la vista de los últimos escándalos. Casos recientes, como el de Facebook, demuestran que no siempre se utilizan como el usuario espera y que, en muchas ocasiones, la actitud de la empresa no se corresponde con la información del usuario al respecto.

Algunas compañías como Facebook ya no son únicamente una red social para compartir con amigos experiencias o contenidos digitales, sino una gigantesca base de datos con un tremendo potencial comunicativo y económico. Lo preocupante de este hecho es la ambivalencia de esa capacidad de las redes, que puede beneficiar o perjudicar a los ciudadanos.

En el Reino Unido, el escándalo de Cambridge Analytica mostró hace unos meses que Facebook habría vendido datos personales de perfiles de millones de usuarios de la red social a terceros —a clientes suyos— con fines comerciales y políticos.

Los usuarios de la red social, como podría pasar con los de otras aplicaciones, no imaginaban que se procesarían sus datos y los de sus amigos con solo descargarse una *app* diseñada por Cambridge Analytica y vinculada a Facebook. Tampoco quedaba claro que, por participar en una encuesta *online* por la que a cada encuestado ingresaba entre dos y cinco dólares, se acabarían procesando sus datos mediante plataformas de inteligencia artificial como «Mechanical Turk» de Amazon.

Quizá lo más grave pudo ser el destino de esas informaciones. A partir de más de 270 000 personas, a través de los «me gusta» y del perfil de los participantes, se recabaron sin su consentimiento los datos personales de todos los encuestados y sus amigos, más de 87 millones de usuarios, según las últimas cifras oficiales. Esos datos se cruzaron con los gustos de los usuarios en Facebook mediante herramientas de *big data* y, luego, con diversos algoritmos, se diseñaron campañas segmentadas y orientadas específicamente a unos dos millones de votantes.

Estas situaciones muestran cómo las redes sociales y las compañías creadoras de aplicaciones no siempre cumplen con las normas que protegen la privacidad de los ciudadanos. Por eso, se han visto abocadas a graves crisis de reputación y credibilidad. Al mismo tiempo que intentan frenar sus incontables pérdidas en bolsa y contener la diáspora de usuarios, han de responder legalmente ante las autoridades en EE. UU. y en Europa.

Pero el problema no es nuevo. Algunos estudios, incluido también uno español de febrero de 2018, han revelado que varias de estas redes sociales usan datos sensibles para la publicidad en Europa sin consentimiento, práctica prohibida por el Reglamento Europeo de Protección de Datos vigente desde 2016. En su artículo 9, este Reglamento menciona los ámbitos más delicados: origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, así como particularidades de salud, genéticas y biométricas.

La información más preocupante, obtenida de estudios rigurosos, es que Facebook, que alberga más de dos mil millones de cuentas en todo el mundo, tiene en su poder los datos sensibles de casi el 40 por ciento de los ciudadanos europeos. Dispone de la información personal de casi 205 millones de europeos de forma no completamente anónima, por lo que la identidad de estos ciudadanos podría ser explicitada mediante los datos archivados en sus servidores, cuestionando y poniendo en grave peligro su privacidad. Sin embargo, lo más llamativo es que Facebook pueda manejar estos datos sensibles sin el consentimiento expreso ni claramente informado de los usuarios.

Sin perjuicio del alcance legal y de las conclusiones finales de las investigaciones que se están llevando a cabo, se trata de situaciones de un riesgo sin precedentes. Además de cumplir la regulación vigente sobre protección de datos, convendría que las redes sociales y servicios en internet asumieran la premisa de que la privacidad está por encima de intereses comerciales o electorales. Los usuarios, por su parte, pueden prestar más atención a los textos informativos de las suscripciones y dar su consentimiento cuando realmente estén seguros de que se les ofrecen garantías suficientes.

Efrén Díaz Díaz [Der 01], abogado del bufete Mas y Calvet. European Data Protection Officer.

LA PREGUNTA DEL AUTOR

¿Lee usted los mensajes sobre la protección de datos que aparecen en las redes sociales antes de inscribirse en ellas?

@NTunav
Opine sobre este asunto en Twitter. Los mejores tuits se publicarán en el siguiente número.