Facebook, ¿otra vez?

Facebook vuelve a ser noticia y, como es habitual, no porque cuente con una nueva funcionalidad para maquillar nuestras fotos o con un nuevo minijuego que nos permita cuidar de animales, pitufos o demás criaturas, sino porque se ha producido un nuevo escándalo relacionado con la filtración de los datos personales tratados por ésta red social. A juzgar por el ruido mediático generado, este puede ser el golpe definitivo para la reputación del gigante californiano.

Javier de Miguel, manager de ÉCIJA.

▶ Pero... ¿qué es eso tan malo que ha hecho Facebook? Para responder a esta pregunta primero debe tenerse en cuenta que Facebook está sometido a la normativa de protección de datos, ya que, según establece el Reglamento General de Protección de Datos (RGPD o GDPR de sus siglas en inglés), cualquier operación o conjunto de operaciones realizadas sobre datos o conjuntos de datos (recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción); que permitan la identificación de una persona física, implica el tratamiento de datos de carácter personal, lo cual conlleva, irremediablemente, el deber de cumplir con lo dispuesto en la normativa de protección de datos aplicable.

En este sentido, Facebook, como responsable del tratamiento de los datos personales de sus clientes (es decir, aquel que decide sobre la finalidad del tratamiento llevado a cabo) debe respetar los principios rectores del tratamiento de datos personales.

Es decir, según el RGPD, Facebook debe tratar los datos de sus usuarios de manera lícita, leal y transparente y para finalidades concretas, explícitas y legítimas. Debiendo, asimismo, tratar exclusivamente datos adecuados pertinentes y limitados para el cumplimiento de dichas finalidades; sólo durante el tiempo necesario para cumplir con dicha finalidad, asegurándose de suprimir aquellos que ya se encuentren desactualizados y garantizando la integridad y confidencialidad de la información.

Pero además de lo anterior, Facebook debe cumplir con las restantes obligaciones establecidas en la normativa. Entre las cuales destacan la de informar de los aspectos relativos al tratamiento de datos que se pretende llevar a cabo, la de obtener el consentimiento del usuario, en los casos en los que sea necesario y la de aplicar las medidas de seguridad técnico-organizativas necesarias para garantizar que no se produzca el acceso no consentido a los datos de los usuarios.

Por lo tanto, Facebook debe poner a disposición de sus usuarios la información suficiente para conocer los aspectos esenciales del tratamiento que se pretende realizar. Información que debe ser clara y transparente, de forma que realmente permita al usuario conocer previamente qué va a hacer Facebook con sus datos y decidir si desea dar su consentimiento para que los mismos sean tratados por la red social o por terceras empresas. En relación a esto último, el hecho de permitir el acceso de un tercero a la información personal tratada supone una comunicación de datos (como así define la normativa al tratamiento que permite que

un tercero, que no sea un prestador de servicios del responsable, acceda a los datos personales tratados) y, por lo tanto, la misma debe ser informada y, con carácter general, consentida por el usuario.

Sin embargo, el deber de evitar que terceros no autorizados accedan a la información personal de los usuarios recae sobre Facebook, por lo que será necesario que la red social cuente con medidas de seguridad eficaces para garantizar que no se produce ningún acceso irregular a los datos de los usuarios.

¿Y no lo ha hecho? Lo cierto es que, a los chicos de Mark Zuckerberg nunca les ha "resultado fácil" cumplir con la normativa de privacidad y protección de datos. Prueba de ello es que Facebook acumula sanciones por vulnerar el derecho a la privacidad y a la protección de los datos de los ciudadanos europeos, al no haber informado debidamente a los usuarios de los tratamientos llevados a cabo, por tratar los datos (incluso especialmente protegidos) sin obtener el correspondiente consentimiento del usuario o por no suprimir los datos de los usuarios cuando así correspondía. De hecho, Facebook es el "ganador" de la sanción más alta en la historia de la Agencia Española de Protección de Datos (AEPD), por importe de 1,2 millones de euros. Pero no resulta tan frecuente que sufra brechas de seguridad, como la ocurrida en el caso del escándalo de Cambridge Analytica.

Según ha sido reconocido por la propia red social, la empresa londinense especializada en minería y analítica de datos, tuvo acceso a los datos de 87 millones de usuarios. Sin embargo, según las últimas manifestaciones realizadas por el alto mando de la compañía, el acceso a la información no se produjo con el beneplácito de la red social, sino que se ha tratado de un robo de información realizado por Cambridge Analytica a través de la aplicación thisisyourdigitallife, que, según se informaba, se empleaba con fines académicos.

> "EL DAÑO REPUTACIONAL SUFRIDO POR LA COMPAÑÍA, PESE AL 'MEA CULPA' DEL SEÑOR ZUCKERBERG, YA ES IRREPARABLE"

En este sentido, el hecho de que la cesión no estuviera prevista y no se hubiera realizado voluntariamente por Facebook (en caso de que esta argumentación efectivamente se confirmase), podría desvirtuar el incumplimiento por Facebook del deber de informar al usuario de la cesión de sus datos a Cambridge Analytica (de hecho, el propio RGPD establece la obligatoriedad de informar al interesado de los destinatarios de dicha información, antes de que se produzca la puesta a disposición de la misma a dichos receptores) y del de obtener su consentimiento para llevar a cabo la cesión de sus datos.

Sin embargo, el escándalo en cuestión evidencia un aspecto fundamental del que, presumiblemente, y siempre partiendo de la información con la que se cuenta en la actualidad, Facebook no tendrá fácil defenderse. El hecho de que Cambridge Analytica haya accedido a los datos de los usuarios de la red social sin el consentimiento de los mismos, permite pensar que las medidas de seguridad tanto técnicas como organizativas con las que cuenta Facebook para proteger la privacidad de sus usuarios no son eficaces.

Es decir, el deber de proteger la privacidad de los usuarios debe entenderse como una obligación de resultado, esto es, aquella que sólo puede tenerse por cumplida cuando se cumple el objetivo pretendido (en este caso, salvaguardar la confidencialidad de la información). Por lo que, el hecho de que una empresa de análisis de datos haya podido acceder a la información de usuarios evidencia que las medidas de seguridad implantadas por la compañía californiana no han sido suficientes. Más si cabe, cuando, las finalidades para las que Cambridge Analytica empleo los datos y de los resultados alcanzados (según parece el tratamiento de esta información sirvió como catalizador para la victoria de Donald Trump y para el éxito del *Brexit*) permite suponer lo sustraído es información agregada muy valiosa, que incluso arroja información de la ideología política de los usuarios.

Diversas autoridades de control, entre ellas la AEPD, han comenzado a investigar el asunto, por lo que en unos meses veremos si Facebook es nuevamente sancionada con una cifra millonaria.

En todo caso, el daño reputacional sufrido por la compañía, pese al "mea culpa" del señor Zuckerberg, ya es irreparable. **CW**