La red social más importante del mundo ha sufrido un serio revés motivado por la filtración masiva de datos de millones de sus miembros a una consultora británica, que los empleó con fines no permitidos. Pese a la pérdida masiva de confianza, sus ganancias el primer trimestre de año han subido más de un 60% y el coste en pérdida de usuarios ha sido moderado.

LUIS MENÉNDEZ

luis.menendez@yahoo.es

¿La crisis de Facebook?

FACEBOOK, LA RED SOCIAL fundada en 2004 y que actualmente cuenta con cerca de 2.000 millones de usuarios, ha afrontado uno de los episodios más negros de su historia. El pasado mes de marzo varios medios de comunicación se hacían eco de que una empresa dedicada a la *minería* y análisis de datos llamada Cambridge Analytica había usado de forma indebida los datos de millones de usuarios de Facebook.

De forma indebida porque Facebook permitía que las aplicaciones que lo solicitaran pudieran recopilar –únicamente con fines de investigación– datos de sus usuarios siempre que estos prestaran su consentimiento para el acceso de dicha *app*, pero la consultora británica los usó con una finalidad no permitida.

A través de la aplicación *thisisyourdigitallife* la empresa accedió a los datos de 87 millones de usuarios de Facebook. Según las primeras informaciones, Cambridge Analytica empleó los datos obtenidos para crear perfiles psicopolíticos –teóricamente para predecir las decisiones de los votantes e influir en ellos– que habrían sido ven-

Derecho al olvido

EL nuevo Reglamento General de Protección de Datos recoge la figura conocida como derecho al olvido. No se trata de un derecho nuevo sino la representación de los tradicionales derechos de cancelación y oposición recogidos en la normativa española de protección de datos. En mayo de 2014, el Tribunal de Justicia de la Unión Europea dictó una sentencia que vino a respaldar el criterio que durante años venía aplicando la AEPD, estableciendo que el tratamiento de datos que realizan los motores de búsqueda está sometido a las normas de protección de datos de la Unión Europea y que las personas tienen derecho a solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre.

"El derecho al olvido se recoge en el Reglamento General en los mismos términos que se reconoció por el TJUE, limitándolo al borrado de los resultados de los buscadores cuando éstos ya no sean actuales o relevantes", explica Adsuara. "Cuando los datos ya no sean necesarios para la finalidad para la que fueron recabados o si su tratamiento vulnera de alguna manera lo dispuesto en la normativa vigente, el prestador de servicios deberá suprimir los datos, lo que no significa que la información vaya a desaparecer de la fuente, solo de las listas de resultados que arroja el buscador", matiza Tejerina.

Otros enfoques, mismo tema

▶ En una entrevista de *Público*, Evgeny Morozov –una de las voces que representa el pensamiento crítico hacia el discurso de Silicon Valley–, aborda la polémica de Facebook y Cambridge Analytica y cuestiona la eficacia del llamado *microtargeting*.
▶ http://cort.as/-58S7

▶ *El País* analiza en este reportaje la precisión con la que se puede determinar nuestro perfil psicológico en internet.
▶ http://cort.as/-58Sl

▶ *El Mundo* recoge en esta noticia las acciones llevadas a cabo por la AEPD en relación con el caso Facebook-Cambridge Analytica.
▶ http://cort.as/-58U6

didos para tratar de impulsar la campaña del entonces aspirante a la presidencia de Estados Unidos, Donald Trump, en las elecciones de 2016.

Sin embargo, "la posible influencia de la conducta de Cambridge Analytica en los resultados de las últimas elecciones en EE.UU. es más que discutible", aprecia Borja Adsuara, experto en Derecho, Estrategia y Comunicación Digital, en alusión a las declaraciones de los miembros de la consultora política y de expertos en *nanotargeting*, que afirman que esta hipótesis no se puede demostrar científicamente.

Mark Zuckerberg: 'No tuvimos una visión lo suficientemente amplia de cuál era nuestra responsabilidad y eso fue un gran error. Fue mi error y lo siento'

En su opinión, la intención de influirnos no está en la tecnología, sino en la publicidad, el marketing y la propaganda. Asume que el *nanotargeting* ofrece más información sobre nosotros, "pero no está tan claro que consigan manipularnos contra nuestra voluntad, sino que nos ofrecen lo que nos interesa, porque conocen mejor los gustos de cada uno". Ante este riesgo –sostiene– lo que se puede hacer es "aplicar la legislación ya existente de protección de datos y, sobre todo, reforzar la educación para formar ciudadanos con pensamiento crítico".

Afectados en España. En el caso de España, 44 personas instalaron *thisisyourdigitallife*, que permitía acceder a la información personal de los usuarios y a la de sus contactos, lo que elevó el número de personas potencialmente afectadas hasta la cifra de 136.985, según las propias estimaciones de Facebook, que realizó el cálculo recurriendo a análisis internos con una 'metodología expansiva'.

Ante la posible vulneración de la normativa, la Agencia Española de Protección de Datos (AEPD) ha abierto actuaciones de investigación a Facebook para analizar la posible afectación de usuarios españoles. De hecho, en los últimos meses la Agencia ha impuesto tres sanciones –de 1,2 millones, 150.000 y 300.000 euros– a esta red social por diferentes incumplimientos de la Ley Orgánica de Protección de Datos.

'Fue mi error y lo siento'. El vendaval mediático levantado por la filtración masiva de datos de millones de miembros, en su mayoría estadounidenses, a la consultora británica y la divulgación de noticias falsas llevó al multimillonario director de Facebook, Mark Zuckerberg, a comparecer en el Congreso de Estados Unidos para dar cuenta de su gestión por estos hechos y responder a las preguntas de los legisladores de dos comisiones del Senado y una de la Cámara de Representantes. Recientemente también acudió al Parlamento Europeo para disculparse y explicar lo ocurrido.

Nueva regulación

UNO de los senadores que dirigió preguntas a Zuckerberg acusó a este de falta de diligencia y de responsabilidad para proteger la información privada de la gente, y mostró su preocupación por la dificultad de la red social de cambiar su modelo de negocio si no es con una regulación concreta. En este sentido, el director de Facebook declaró estar "abierto a debatir y negociar estos aspectos", a una mayor regulación, incluso similar al nuevo marco europeo de protección de datos.

"Está claro ahora que no hicimos lo suficiente para prevenir que estas herramientas fueran usadas para hacer daño. Esto se refiere a las noticias falsas, la interferencia extranjera en elecciones, el discurso del odio y la privacidad de datos", señaló Zuckerberg. "No tuvimos una visión lo suficientemente amplia de cuál era nuestra responsabilidad y eso fue un gran error. Fue mi error y lo siento. Comencé Facebook, lo administro y soy responsable de lo que sucede allí", añadió. Además, reconoció que su compañía reaccionó "de manera lenta" a la supuesta injerencia de Rusia en las elecciones estadounidenses de 2016.

La punta del iceberg. El escándalo de Cambridge Analytica ha puesto de relieve que este caso podría ser solo la punta del iceberg. Esta sospecha fue formulada a Mark Zuckerberg por uno de los legisladores. "Además del robo de datos de Cambridge Analytica, ¿conoce otros casos en los que terceras compañías hayan robado datos? Y si es así, ¿cuántos casos?" Su respuesta no fue lo que se dice tranquilizadora: "Estamos investigándolo, puede haber decenas de miles de aplicaciones que hayan accedido de forma ilegal a los datos. En cuanto lo sepamos y tengamos los datos, haré que mi equipo se los facilite".

Borja Adsuara: 'La posible influencia de la conducta de Cambridge Analytica en los resultados de las últimas elecciones en EEUU es más que discutible'

Ofelia Tejerina, abogada y miembro del Grupo de expertos sobre derechos digitales del Ministerio de Energía, Turismo y Agenda Digital, considera que "hoy nadie es tan ingenuo como para pensar que los desarrolladores de *apps* o los proveedores de servicios de internet no utilizan los datos de sus usuarios casi como les viene en gana, a veces saltándose las leyes a veces bordeándolas, aprovechando lagunas o la existencia de fronteras legislativas, todo ello, en tanto la tecnología les permite hacer perfiles con mucha precisión". Para Tejerina, la gran preocupación es lo que hacen con esos datos y si existe o no la posibilidad real de obtener pruebas para exigirles responsabilidad.

Todo sigue igual. Más allá de la pérdida masiva de confianza, Facebook no parece haber acusado el golpe en lo que a ganancias y pérdida de usuarios se refiere. Así, el gigante tecnológico ha anunciado que las ganancias entre enero y marzo de 2018 subieron un 63% respecto a 2017 y se situaron en 5.000 millones de dólares, mientras que el volumen de negocio subió un 49%, a 11.970 millones de dólares.

La pérdida de confianza tampoco parece haberse traducido en pérdida de usuarios. Una encuesta realizada por Ipsos entre el 26 y el 30 de abril refleja que el impacto del filtrado de datos personales ha afectado de forma moderada a la compañía, ya que solo uno de cada cuatro encuestados asegura haber reducido su actividad en Facebook e incluso haber cerrado su cuenta. ●

VÍCTOR DOMINGO,
presidente de la Asociación
de Internautas

presidente@internautas.org
www.facebook.com/victor.domingo
@victordomingo
http://www.internautas.org

¿Podemos controlar nuestros datos?

LOS ESCÁNDALOS DE FACEBOOK y Cambridge Analytica han sido una llamada de atención sobre la falta de respeto generalizada a la privacidad de millones de ciudadanos. Un problema global. La gente de todo el mundo está preocupada por la explotación de sus datos. La actual falta de transparencia sobre cómo las empresas están utilizando los datos de las personas es inaceptable y de alguna manera nos deja en la más absoluta indefensión.

Existe todo un ecosistema oculto de compañías que recolectan y comparten datos personales. Desde que entramos en un centro comercial con nuestro *smartphone*, un dispositivo que no solo sirve para hablar por teléfono o *guasapear*. Además, incluye por defecto almacenar nuestros datos, fotografías, cuentas de nuestros sitios en internet; vamos, un auténtico alijo de información personal que, si no desactivamos el WIFI y Bluetooth cuando llegamos al centro, ponemos a disposición de cuantas empresas dedican sistemas de localización, identificación y segmentación de todos los que pasamos por allí, incluso sin conectarnos a las WiFi's gratuitas que ponen a disposición del público. Lo más seguro es desconectar, dejar el dispositivo apagado en el coche y disfrutar del placer de comprar con su privacidad puesta a salvo.

Pero no solo las empresas persiguen nuestros datos, los gobiernos también. Un reciente informe desvelado por Human Rights Watch, afirma que las autoridades chinas han puesto en marcha en la provincia de Xinjiang un auténtico Minority Report, un programa de vigilancia predictiva. El programa agrega datos sobre personas, a menudo sin su conocimiento, y señala a los que considera potencialmente amenazantes para los funcionarios. Aquellos son detenidos en función de esas predicciones y enviados a "centros de educación política" extra legales donde permanecen indefinidamente sin cargos ni juicio alguno. Desde agosto de 2016, la Oficina de Seguridad Pública de Xinjiang ha publicado avisos de adquisiciones que confirman el establecimiento de la "Plataforma integrada de operaciones conjuntas" –IJOP– un sistema que recibe datos sobre personas de diferentes fuentes.

Estos avisos revelan que el IJOP recopila información de múltiples fuentes o "sensores". Una fuente son las cámaras de CCTV, algunas de las cuales tienen reconocimiento facial o capacidades de infrarrojos (dándoles "visión nocturna"). Algunas cámaras se colocan en lugares que la policía considera sensibles: lugares de entretenimiento, supermercados, escuelas y centros religiosos. Otra fuente es el *sniffers wifi*, que recoge las direcciones de identificación únicas de computadoras, teléfonos inteligentes y otros dispositivos en red. El IJOP también recibe información como números de matrículas y números de tarjetas de identificación de ciudadanos de algunos de los innumerables puntos de control de seguridad de la región y de los "sistemas de gestión de visitantes" en las comunidades controladas por el acceso. Los puntos de control del vehículo transmiten información a IJOP y "reciben, en tiempo real, advertencias predictivas impulsadas por el IJOP" para que puedan identificar objetivos... para un riguroso control de los ciudadanos. No solo se viola el derecho a la privacidad sino que también permite a los funcionarios detener arbitrariamente a las personas. En este caso, la realidad está superando a la ficción.

Ante este sombrío panorama contra la privacidad, en España ha entrado en vigor el pasado 25 de mayo el nuevo Reglamento General de Protección de Datos (RGPD) que sustituirá a la actual normativa. Está teniendo un periodo de adaptación de dos años, periodo para que las empresas y organizaciones adapten sus términos y condiciones así como para que den a conocer estos cambios a sus usuarios. Se abre una cierta esperanza para garantizar el control de nuestros datos por parte de empresas e instituciones y por supuesto, por la propia ciudadanía.

«La actual falta de transparencia sobre cómo las empresas están utilizando los datos de las personas es inaceptable y de alguna manera nos deja en la más absoluta indefensión»

Cabe destacar que, a partir de esa fecha, podremos solicitar que nuestros datos desaparezcan de la base de datos de determinados registros cuando estos ya no sean necesarios para la finalidad con la que fueron recogidos o cuando hayan sido recogidos de forma ilícita. Además, podremos solicitar que se bloqueen en las listas de resultados de los buscadores enlaces a información obsoleta, incompleta, falsa o irrelevante. Por otro lado, también tendremos derecho a solicitar la recuperación de los datos para poder ser transferidos a otro responsable. Junto con los derechos que ya conocíamos de acceso, rectificación, cancelación y oposición, se regula el ya conocido derecho al olvido, se amplía el derecho a la portabilidad de los datos y se reconoce el derecho a la limitación en el tratamiento.

El nuevo reglamento que acaba de entrar en vigor puede ayudarnos a crear protecciones globales muy necesarias para proteger nuestros datos y por ende garantizar el control de los mismos. Es necesario que aprobemos esta asignatura pendiente que no es otra que hacer respetar y respetar nosotros mismos el uso y gestión de nuestros datos personales y por añadidura, hacer prevalecer el derecho fundamental a la privacidad de nuestros datos y comunicaciones.

"La falsificación digital añade valor a la autenticación y a la acreditación por terceros"