¿Quién comparte mis datos?

CONSCIENTES O NO, CADA VEZ que encendemos el ordenador o cogemos un *smartphone* estamos dando pistas a las empresas sobre nuestros intereses, necesidades y gustos. Si además realizamos compras *online*, contratamos servicios domésticos y nos descargamos aplicaciones gratuitas, el control sobre nuestros datos personales se debilita. Por eso, los expertos advierten del riesgo que suponen las nuevas tecnologías cuando no se manejan con el conocimiento suficiente y de manera responsable. Se trata, simplemente, de proteger nuestra privacidad y ejercer un control necesario sobre la información que aportamos a las empresas que manejan nuestros datos, pero también a los miles de ciberdelincuentes que campan por la Red. "No se trata de demonizar internet sino de hacer un uso positivo y consciente", señala Víctor Domingo, presidente de la Asociación de Internautas, quien tampoco es partidario de una red anónima que evite a los ciudadanos ser identificados, sino de una red en la que estos estén mucho más protegidos y seguros.

Los ciudadanos tenemos que ser más responsables en el uso de las redes sociales y las plataformas digitales

¿Con o sin consentimiento? El problema empieza cuando esos datos se utilizan sin el consentimiento del usuario o cuando se ceden a terceros, una práctica mucho más habitual de lo que creemos y que no siempre se realiza dentro de la legalidad. La alarma social saltó hace tres años tras la compra de la aplicación de mensajería WhatsApp por parte de la red social Facebook y la posibilidad de que este tipo de compañías cruzara los datos de usuarios con fines diversos. Aunque en un prin-

Los datos se han convertido en el gran filón para las empresas que buscan obtener de ellos nuevas ventajas competitivas. Almacenar, analizar y gestionar datos de manera eficaz es hoy el gran reto de los profesionales del marketing. Sin embargo, los expertos advierten del coladero que suponen internet, las redes sociales y las aplicaciones móviles para obtener información de los consumidores, en un mercado en el que existen ciertas grietas legales. Mientras llegan las mejoras prometidas en el nuevo Reglamento Europeo de Protección de Datos que será plenamente aplicable en mayo de 2018, los expertos recomiendan responsabilidad y estar alerta ante cualquier práctica dudosa que detectemos.

MARIÁN LEZAUN
marianlezaun@gmail.com
@mlezaun

Cada vez que encendemos el ordenador o cogemos un *smartphone* estamos dando pistas a las empresas sobre nuestros intereses, necesidades y gustos

cipio Facebook negó esta práctica, tiempo después cambiaba su política de privacidad y ofrecía a sus usuarios la vinculación de identidades entre las dos plataformas. A Facebook, la treta le ha salido cara y la Comisión Europea le ha impuesto una multa de 110 millones de euros por ocultar información y saltarse las condiciones del acuerdo de fusión. Sin embargo, para Domingo, el gran reto no está tanto en sancionar a las grandes empresas como en compensar a los usuarios. "Para este tipo de compañías una multa económica no supone ningún problema, mientras el usuario, que es la verdadera moneda de cambio de la operación comercial, no recibe ninguna compensación."

Siempre alerta. Así, cada vez que damos nuestros datos personales, es decir, aquella información que puede revelar nuestra identidad en cualquier ámbito, debemos

Para saber más

La Agencia Española para la Protección de Datos ofrece en su web una guía para conocer todos nuestros derechos y obligaciones como ciudadanos respecto al tratamiento de nuestros datos. Entre ellos el derecho al olvido, la portabilidad o la eliminación de la publicaciones.
▶ http://cort.as/yedl

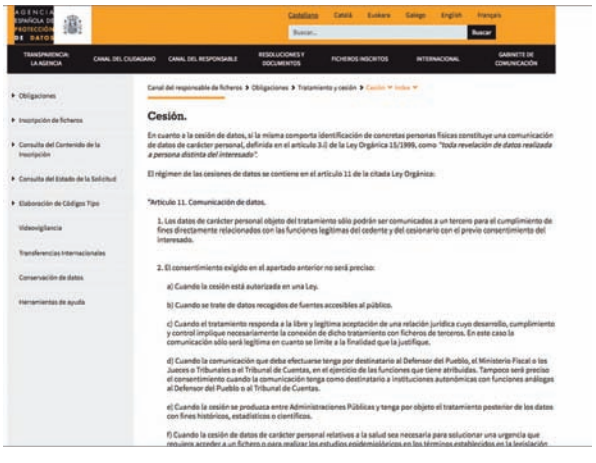
La organización europea de consumidores (BEUC) reclama mayor protección sobre los datos de los consumidores, expuestos de manera continua a lo que las empresas quieran hacer con ellos.
▶ http://cort.as/yTRV

La Asociación Profesional Española de Privacidad (Apep) cuenta en su página web con todas las novedades que afectan a la protección de datos, así como con entrevistas a las principales autoridades en la materia.
▶ http://cort.as/yTfC

La Asociación de Internautas ha elaborado una guía con los conceptos clave para poder navegar de manera segura y utilizar las redes sociales de manera correcta. La guía se dirige tanto a las personas adultas como a los menores.
▶ http://cort.as/yTeR

¿Existen excepciones a la cesión de datos?

La Ley Orgánica de Protección de Datos contempla ocho excepciones a la cesión de datos entre empresas. Para empezar, cuando esa cesión de datos la autorice una norma con rango de Ley. Es decir, cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Se pueden ceder también cuando se trate de proteger el interés vital del interesado o cuando los datos figuren en fuentes accesibles al público y no en todo caso. Solo en los supuestos de satisfacción de un interés legítimo, por parte del responsable del tratamiento o por el tercero a quien se comuniquen los datos, y sin vulnerar los derechos y libertades fundamentales del interesado. La Ley contempla, además, la cesión que responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos.



▶ http://cort.as/yfGP

La alarma social saltó tras la compra de WhatsApp por la red social Facebook y la posibilidad de que estas compañías cruzaran los datos de sus usuarios

tomar ciertas precauciones. Mònica Vilasau Solana, profesora de los Estudios de Derecho y Ciencia Política en la Universidad Oberta de Catalunya y experta en protección de datos advierte de que, "en el momento en el que rellenamos un cuestionario debemos ser conscientes de que ya perdemos el control sobre los mismos, especialmente cuando esos datos se introducen en internet". No obstante, propone una serie de recomendaciones para estar más protegidos. "En primer lugar, es preciso leer bien la información que se proporciona, especialmente quién es la persona (física o jurídica) que tratará los datos que introducimos y con qué finalidad; para saber si estamos o no de acuerdo con dicha finalidad y si deseamos proporcionarlos realmente", explica. Según la Ley Orgánica de Protección de Datos, los datos requeridos por una empresa deben de usarse para una finalidad determinada y el sujeto que los trata debe de estar bien identificado. "Sin embargo hay que estar atento a las posibles cesiones de los datos a otros sujetos o empresas." Para Vilasau, la realidad es que, una vez proporcionamos los datos, de alguna forma perdemos su control, aunque no por ello debemos pasar por alto nuestros derechos como consumidores. "Tenemos derecho a ser informados, a acceder a nuestra información y saber si se han hecho ulteriores cesiones, revocar el consentimiento otorgado en cualquier momentos y pedir la supresión de los datos en determinadas circunstancias", apunta esta experta.

En el mismo sentido, Cecilia Álvarez, presidenta de la APEP (Asociación Profesional Española de la Privacidad), insiste en que "debemos de leer la política de privacidad o de protección de datos de las compañías, comprobar quién es la entidad que se identifica como responsable y ver la finalidad que dará a esos datos". Para Álvarez, elegir las entidades con las que nos vamos a relacionar en función de su política de privacidad es clave, al igual que las elegimos por sus condiciones comerciales o su compromiso social. Según Álvarez, "los consumidores tendemos a pensar que no ser responsables de nuestros datos es problema de otros, cuando en realidad, no es así".

Por eso, para los expertos, la información es clave y nuestro comportamiento responsable, también. En principio, según ha señalado la Agencia Española de Protección de Datos, internet no es un medio de comunicación, por lo que no puede llevarse a cabo un uso indiscriminado de los datos que se hallan en la Red. Pero una cosa es lo que establece la normativa y otra su cumplimiento. En consecuencia, ante un uso indebido de nuestros datos, no siempre será fácil identificar el responsable del mismo. "Además, la Red no conoce fronteras jurídicas. Si los datos se hallan en servidores ubicados en países que no tienen un nivel similar de protección al nuestro, y a pesar de que la normativa europea sea vinculante y aplicable, difícilmente se podrá hacer efectiva una reclamación", señala Vilasau.

Para muchos usuarios existe la incertidumbre de si todas las empresas que operan se ajustan a la normativa española.

Para muchos usuarios existe, además, la incertidumbre de si todas las empresas que operan se ajustan a la normativa española. Una cuestión que no es tan sencilla como parece: "De hecho cumplir con la normativa en su totalidad es muy complejo. Puede afirmarse que cada vez existe una mayor cultura de que debe cumplirse con la normativa, quizá, entre otras razones, por el elevado coste económico que representa no hacerlo", reconoce Vilasau.

Así las cosas, solo queda seguir ciertas normas. "Conviene disponer de una firma electrónica, de utilizar contraseñas robustas, de confiar solo en páginas web que cumplan con las políticas de privacidad, usar pasarelas de pago, etcétera", recomienda Domingo. ●

¿Dónde acudir en caso de sospecha?

Si creemos que estamos sufriendo un uso indebido de nuestros datos, en primer lugar debemos acudir a la entidad que consideramos responsable del abuso. En la mayoría de las ocasiones, el *spam* (correos no deseados) o la aparición en ficheros comerciales o listas de morosos, por ejemplo, son la pista seguida por los usuarios. Si en el plazo previsto dichas empresas no responden a nuestra reclamación debemos acudir a las autoridades de protección de datos, tanto autonómicas como a la Agencia Española de Protección de Datos, que es nacional; son las encargadas de tramitar los procedimientos sancionadores.

MIGUEL PÉREZ SUBÍAS,
presidente Congreso Europeo de Privacidad y Protección de Datos

www.congresodeprivacidad.com

Por qué es cada vez más importante la privacidad de los datos personales

LA PRIVACIDAD ES EL DERECHO QUE tenemos las personas a mantener en la esfera privada una parte de lo que hacemos, decimos o pensamos y el derecho a decidir qué parte de ese espacio privado queremos compartir y con quién queremos compartirlo. La Real Academia define la privacidad como "el ámbito de la vida que se tiene derecho a proteger de cualquier intromisión" un derecho por cierto recogido en las constituciones de muchos países y en la Carta de Derechos Fundamentales de Naciones Unidas.

El nivel de preocupación por la privacidad, de los usuarios de internet, es bajo ya que en general confiamos en el ecosistema. El ciudadano normal desconoce quién o quiénes tienen acceso a sus datos, cómo se recolectan, para qué se usan, para qué se podrían usar y su valor económico. Sin embargo valoramos nuestra privacidad y hay una corriente creciente en las sociedades más avanzadas en materia de derechos que empieza a preguntarse sobre dónde están los límites de la tecnología proponiendo nuevas regulaciones en esta materia.

La tecnología está cambiando el paradigma de la privacidad en primer lugar por la cantidad de datos personales que se generan y que se almacenan cada día en un ente abstracto que llamamos internet o la nube.

Cada año y medio se generan más datos que en toda la historia de la humanidad. Hoy casi todo lo que hacemos deja una huella de información: el uso de nuestro móvil, la consulta de un mapa, un viaje, un comentario compartido en una red social, una opinión en un blog, un pago con tarjeta de crédito o nuestro uso de energía detallada en los *smartmeters*, entre otros.

Los datos personales cada vez son más importantes para el desarrollo de los nuevos servicios digitales cada vez más personalizados y cada vez más adaptados a lo que somos, hacemos y decimos. Cada vez son más las aplicaciones y servicios que requieren de datos personalizados y cada vez son más los dispositivos, sistemas y aplicaciones que recogen datos personales.

Para mayo de 2018 todas las empresas que tengan datos personales de ciudadanos de la Unión Europea deberán cumplir con las nuevas normas de privacidad conocidas como el Reglamento General de Protección de Datos (RGPD). La sanción por infracción de los principios recogidos en el RGPD pueden conllevar multas de hasta 20 millones de euros o del 4% del volumen de negocios global anual de la organización. Para otras infracciones de privacidad, las sanciones pueden llegar a los 10 millones de euros o el 2% del ingreso anual de la empresa.

En paralelo con el nuevo RGPD y con la nueva norma (Privacy Shield) para las empresas americanas que procesan datos de ciudadanos Europeos, la UE debate la directiva ePrivacy que introduce cambios importantes en materia de privacidad. Y no solo es Europa la que está regulando esta materia, China y Singapur también están introduciendo nuevas regulaciones con elevadas multas en caso de incumplirlas.

Nos encontramos en un momento en el que hay dos intereses que se contraponen; por un lado el interés económico derivado de la explotación comercial, y por otro los marcos normativos que rigen la protección de datos y la posibilidad de que en algún momento se contravenga alguna de las regulaciones vigentes en esta materia y que esto pueda traernos problemas económicos, de imagen o personales para los directivos implicados.

Las empresas tienen primero que tomar conciencia de la nueva situación en materia de privacidad, comenzar por estudiar la regulación que nos viene (RGPD, ePrivacy y Privacy Shield), y empezar a planificar para cumplir con sus requisitos.

En muchos casos va a ser necesario contratar a un responsable de protección de datos (DPO); cambiar las bases de datos que almacenan datos personales; crear el procedimiento para notificar cualquier infracción dentro de las 72 horas posteriores al descubrimiento, o hacer evaluaciones de riesgo asociado a la pérdida o robo de datos personales.

La forma en la que se informa a los ciudadanos y cómo se recoge el consentimiento también cambia radicalmente. Ya no vale con presentar unas largas y farragosas condiciones de uso que nadie se lee; ahora hay que hacer que sea sencillo, entendible y explícito para que todos los ciudadanos entiendan lo que confirman.

«Cada año y medio se generan más datos que en toda la historia de la humanidad. Hoy casi todo lo que hacemos deja una huella de información»

En primer lugar hay que empezar con el inventario de los datos personales que se manejan en una organización. Hay que tener muy claro cómo se usan y cómo se gestionan; qué datos personales se recogen; quién tiene acceso a estos datos; si los fines del tratamiento de dichos datos personales se ajustan a la legalidad; dónde y cómo se mantienen; cuánto tiempo dichos datos personales se guardan, y cómo se destruyen. Sin olvidar los datos que se ceden a proveedores, y la deslocalización o el intercambio de datos con servicios y aplicaciones de otros países.

Poner a alguien a cargo de este tema. Hay que tener en cada organización a un responsable de protección de datos DPO. Entre sus responsabilidades deberá asegurar el cumplimiento de la regulación; implementar políticas y procesos para el manejo de datos personales; llevar a cabo evaluaciones de impacto, y mantener la documentación obligatoria, entre otros requisitos.

Llevar a cabo ejercicios de evaluación de posibles riesgos de protección de datos y poner en marcha medidas de mitigación le puede exigir desarrollar de forma regular auditorias y pruebas de penetración.

Se trata en definitiva de incorporar la protección de datos en la cultura de su organización y en todos los niveles de la misma, lo cual implica mantener a los empleados, directivos y proveedores informados sobre los procesos y políticas en materia de protección de datos personales.