

## ATENCIÓN EMPRESAS: MIS DATOS SON MÍOS

19 de marzo de 2017

### **La UE endurece en 2018 las multas por uso indebido de información personal**

Es el último ejemplo de cómo algunas corporaciones violan sistemáticamente la privacidad de sus usuarios. “¿Dónde está el límite?”, se pregunta un estudio que acaba de publicar KPMG. Consumidores de 22 países, entre ellos España, demostraron que están muy preocupados por cómo se mercantiliza su privacidad y comienzan a sentirse realmente irritados con actitudes que antes toleraban, aunque sean legales.

El 55% de los consultados en España (el mayor porcentaje de los países participantes) siente, por ejemplo, que no tiene “ningún tipo de control” sobre el uso que las empresas hacen de sus datos, seguidos de franceses y rusos. A escala global, el 60% de la muestra admite que ya borra las cookies en su navegador, más de la mitad gestiona los parámetros de privacidad de sus redes sociales (en España el 46%) y otro 25% recurre a la encriptación, algo que en España solo hace el 18%. El estudio contenía preguntas como “¿qué le parece que tras escribir un correo a un amigo con un plan para viajar a París aparezcan anuncios de hoteles o restaurantes en esa ciudad al navegar?” o “¿acepta que una valla publicitaria electrónica le salude con su nombre propio, le pregunte si ha disfrutado del desayuno y le muestre un anuncio de sus cereales favoritos?”. La respuesta mayoritaria es un “no” a tolerar este tipo de usos. De forma abrumadora, los consultados también rechazan algo que ocurre todos los días: que las aplicaciones accedan a fotos, contactos o historial de navegación. Sin embargo, las cosas cambian cuando hay regalos de por medio. “¿Aceptaría una tablet gratuita a cambio de que una empresa haga un seguimiento de cuándo, cómo y por qué la utiliza?” tiene una buena aceptación, al igual que una propuesta de descuentos al comprar un televisor que monitorice los gustos en un hogar.

El equilibrio, según los expertos, es la clave de esta relación, y por ahora el partido lo ganan las empresas. La OCDE estima que los datos personales de cada usuario reportan casi cinco dólares anuales a Facebook. Pablo González, socio de Deloitte Digital, calcula que existen perfiles por los que se llegan a pagar 90 euros por contacto: “Un correo electrónico puede valer unos 50

céntimos. Otro ejemplo es el perfil de un usuario que esté buscando un seguro, que puede alcanzar los 50 euros; o el que busca una hipoteca, que puede llegar a 250. Los mayores pagos están condicionados a una contratación efectiva”. Incluso hay empresas, como Datacoup, que ofrecen a sus clientes recuperar el poder sobre sus propios datos, algo así como recomprarlos para disponer en exclusiva de ellos. “Tiene que haber una proporcionalidad”, cree Marc Martínez, socio responsable de Ciberseguridad de KPMG. Mientras que para los consumidores españoles la comodidad es más valiosa que el control de su intimidad (53%), en la gran mayoría de países lo segundo ya prima sobre lo primero (con porcentajes entre el 60% y el 87%). “Sin embargo, puede ser demasiado tarde para que los consumidores recuperen el control de sus datos, aunque quieran”, creen en KPMG. La información ya está diseminada y es muy difícil dar marcha atrás. “No es complicado imaginar un futuro no muy lejano en que los datos se empaqueten y negocien en el mercado de valores, donde la información sobre los consumidores más acaudalados tendrá mayor valor”, analiza la consultora. Aunque las personas siguen sin ser conscientes de la cantidad de datos que las empresas tienen de ellas ni el efecto que ocasiona a sus vidas, las cosas comienzan a cambiar. En mayo de 2018 entrará plenamente en vigor el Reglamento Europeo de Protección de Datos, que establece sanciones por incumplimiento de hasta 20 millones o hasta el 4% de la facturación anual.

### **Leyes preventivas**

Ana López Carrascal, directora de Regulatorio, Administrativo y Competencia en KPMG Abogados, admite que España ya tiene “una de las legislaciones más avanzadas de la UE [la Ley de Protección de Datos de 1999]”, pero explica que la nueva norma “pretende cambiar la manera de ver y entender la privacidad, pasando de un enfoque reactivo a uno preventivo”. A partir de ahora, las organizaciones “pasan a ser responsables de analizar sus riesgos y diseñar medidas apropiadas a ellos”. Para Pablo González, las empresas piensan que manejar datos se considera “como un pasivo”, sobre el que se tienen que adoptar “medidas defensivas dependiendo de los desafíos que vayan surgiendo”. Una idea frente a la que propone que se adopten “medidas previsoras para proteger la privacidad de la información. De esta forma, la protección de datos se convierte en un activo de la compañía y en un argumento de venta para los clientes”.

Las empresas, según Marc Martínez, no están haciendo un uso masivo de los datos porque en muchos casos los almacenan en lugares distintos, o en plataformas que no se comunican entre sí. “Se requieren expertos que sepan trabajar con datos, hay grandes carencias en arquitectos de big data”. En suma, muy pocas empresas han invertido en el talento, las plataformas y los procesos para transformar la información que poseen. Además, se necesitan códigos éticos internos que terminen con larguísimos e incomprensibles

contratos (disclaimers) sobre política de privacidad que nadie lee. Hacer inventario de datos, tener sistemas de seguridad sólidos o ser transparentes a la hora de comunicarse con los clientes son consejos que las empresas tienen que empezar a interiorizar a menos que quieran que sus usuarios les den la espalda.

*Fuente: [www.elpais.com](http://www.elpais.com)*