# ASÍ PONEN EN PELIGRO LAS EMPRESAS ESPAÑOLAS TUS DATOS

1 de marzo de 2019

Solo hace 9 meses que entró en vigor el nuevo Reglamento General de Protección de Datos europeo (más conocido como RGPD o GDPR por sus siglas en inglés) y en ese tiempo ya ha puesto patas arriba nuestra forma de utilizar internet y controlar los datos personales. **Tanto por parte de las empresas como de los usuarios**. Pero aún nos quedan puntos de esta normativa por analizar.

Entre las nuevas obligaciones que ha impuesto a las compañías esta legislación están la de decirte qué datos tuyos tienen recopilados o la de pedirte permiso de manera clara cada vez que vayan a recopilar algún tipo de información personal. Una amalgama de deberes que ha cambiado los procesos empresariales y entre los que también se encuentran **normas de ciberseguridad** que obligan a toda empresa que registre una brecha de seguridad que ponga en peligro datos personales a notificar a la autoridad competente (en España es la Agencia Española de Protección de Datos) dicho problema. Y es ahí donde, en el caso patrio, acabamos de encontrar una cifra bastante llamativa.

Desde El Confidencial, gracias a una solicitud de información a través de la Ley de Transparencia, hemos tenido acceso a la cifra exacta de notificaciones recibidas por la AEPD en los meses que lleva en funcionamiento la nueva ley. En total, a fecha de 30 de enero, son **625 avisos de violaciones de seguridad** de los datos personales en 274 días, lo que equivale a más de dos fallos diarios y casi 70 al mes.

A primera vista cualquiera diría que **se trata de un número bastante alto**.

Esto significa que las empresas españolas sufren peligrosos fallos de ciberseguridad a diario y ponen en peligro la información que los usuarios les confían. Pero el análisis no es tan sencillo. La polémica llega mucho más lejos y tiene que ver con la redacción de la norma que, en este caso, deja espacio, quizá demasiado, a la interpretación y a que las empresas jueguen con estos problemas.

## ¿Son muchas o pocas brechas?

Estas notificaciones están reguladas por los artículos 33 y 34 del RGPD y es ahí donde encontramos todos los detalles sobre **qué tipo de brechas deben ser señaladas**, cómo se debe notificar el fallo o sobre las medidas a seguir después de informar de lo sucedido. Hay puntos muy estrictos como las 72 horas que la norma te da para mandar la información a la AEPD, pero hay otros más polémicos, como el que explica en qué casos el fallo debe ser elevado a las autoridades.

La norma dice que esto no se deberá hacer si la empresa decide que es "**improbable que dicha violación de la seguridad constituya un riesgo** para los derechos y las libertades de las personas físicas". ¿Quién evalúa esa probabilidad? Pues es responsabilidad total de la empresa.

La redacción deja tal espacio a la interpretación que, preguntados por este periódico, ni dos abogados expertos en tecnología como Sergio Carrasco y Samuel Parra se ponen de acuerdo en el análisis de la cifra registrada por la AEPD. Para uno es un número demasiado bajo y para el otro demasiado alto.

Carrasco, por ejemplo, **cree que la cifra dada por la AEPD es baja** con respecto al total de incidentes de seguridad que registran anualmente entidades públicas como el Instituto Nacional de Ciberseguridad (en 2017 el INCIBE llegó a resolver hasta 123.000 incidentes, eso sí, sin distinguir entre los que afectaban a datos personales y los que no) y explica que podrían existir muchos más fallos ocultados por las propias compañías. "Es posible que las empresas oculten las brechas por miedo a las sanciones o que ni siquiera sepan que la han sufrido. Es más, puede que incluso sabiendo del fallo no sepan que deben notificarlo o cómo deben hacerlo", apunta Carrasco.

Todo lo contrario opina Parra que asegura que sería muy preocupante si estas 625 notificaciones fueran brechas reales. Cree que es un número altísimo y piensa que se ha inflado por el desconocimiento de las empresas.

"Seguramente varios de esos avisos se dieran **por miedo a las sanciones** sin saber si la brecha ha comprometido seriamente datos personales que ponen en peligro los derechos y las libertades de sus dueños", apunta.

En lo que sí coinciden ambos expertos es en que existe un desconocimiento claro en las empresas sobre este asunto, incluso nueve meses después del aterrizaje de la normativa. Faltan datos y detalles que den más contexto a este número, pero queda patente que **la ciberseguridad es un tema clave** para las empresas españolas y, por tanto, para los usuarios.

*Fuente: www.elconfidencial.com*