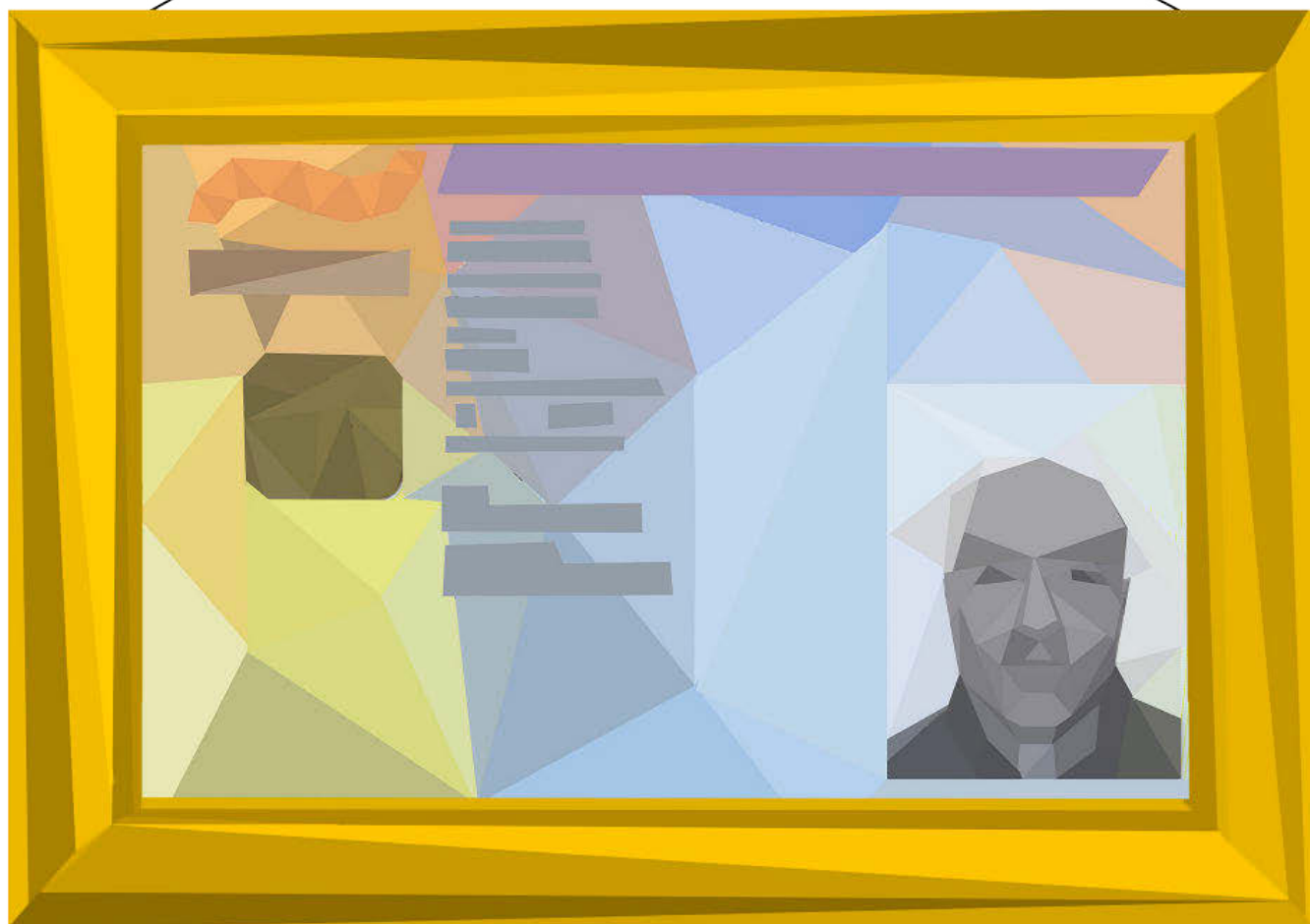




INFORMACIÓN PERSONAL... A LA VISTA DE CASI TODO EL MUNDO

LA CONECTIVIDAD AMENAZA LA PRIVACIDAD DE LOS USUARIOS. REDES SOCIALES Y OPERADORAS DE TELEFONÍA SON LAS COMPAÑÍAS EN LAS QUE MÁS EXPUESTOS ESTÁN LOS DATOS

POR NOELIA MARÍN



Aceptar las *cookies* de manera automática o guardar los datos de la tarjeta de crédito en cualquier *ecommerce* para agilizar futuras compras son acciones habituales y algunos de los errores más comunes que pueden poner en peligro los datos de los usuarios. La conectividad es cada vez mayor, el uso del *smartphone* y los servicios digitales aumenta año tras año y eso hace que la información personal esté más expuesta que nunca.

En opinión de Sergio Maldonado, cofundador y CEO de Privacy

Cloud, empresa de gestión de datos personales, falta concienciación sobre el uso que los portales de Internet hacen de los datos de carácter personal de sus usuarios. "Vamos como kamikazes con nuestros datos. La gente vive con urgencia y ningún usuario se para a leer tres segundos las políticas de seguridad, y aceptan términos y condiciones de aplicaciones y *webs* todo el tiempo sin reflexionar lo más mínimo", explica.

En diciembre se cumplió un año de la entrada en vigor de la *Ley de Protección de Datos Personales y Garantía de los Derechos Digitales*, la trasposición a la normativa nacional del Reglamento General de Datos de la UE. Esta ley obliga a las empresas, entre otras cosas, a contar con el consentimiento expreso de los usuarios para poder ceder sus datos, así como a informarles sobre qué van a hacer con ellos. También exige que avisen cuanto antes a la Agencia Española de Protección de Datos (AEPD) en caso de sufrir un ciberataque.

Hay compañías que ya se han enfrentado a multas por incumplir la legislación, aunque en España las sanciones son inferiores a las de otros países. Entre las multas más recientes destacan casos como el de Vueling, condenada a pagar 30.000 euros por no definir bien sus *cookies*, o RTVE, sancionada con 60.000 euros por perder varios *pen-drives* con datos de 11.000 trabajadores. Ambas sanciones, sin embargo, están lejos de los 204 millones de euros que impusieron a la aerolínea British Airways en

Reino Unido tras el robo de los datos personales de sus clientes.

Según Iván Sánchez, director del Área de Compliance de Garrido Abogados, la imposición de estas multas ha despertado "miedo" en muchas compañías, sobre todo, entre las pymes. "Tienen pavor a enviar correos sin cumplir las normas o cometer un error que les pueda suponer una sanción económica que afecte a sus cuentas, porque no cualquier pyme puede pagar sanciones de decenas de miles de euros sin cerrar", expone.

INFORMACIÓN SENSIBLE. Cuando se habla de robo de datos no toda la información tiene el mismo valor. Según los informes de brechas de seguridad de la AEPD, la información sobre salud, vida sexual, opinión política o raza es la más sensible ante un ciberataque. "Los datos bancarios son valiosos, pero la salud lo es más. El hecho de sufrir una enfermedad crónica o haber sido víctima de cualquier tipo de violencia son cosas que se quedan contigo de por vida y esa información te puede cerrar puertas a la hora de buscar un trabajo", señala Óscar Lage, profesor de ESIC y jefe de Ciberseguridad de Tecnalia. Y lo mismo ocurre con los datos relacionados con la religión o la orientación sexual, "que en caso de hacerse públicos te pueden jugar malas pasadas estando de viaje en determinados países", recalca.

De todas las categorías de datos personales sensibles, la salud es la que más brechas de seguridad experimenta. El origen de la pérdida de datos puede ser un *hackeo*, "pero también un médico que se deja un USB olvidado en un sitio público o una enfermera que pierde un móvil", apunta Maldonado.

Pero, ¿qué tipo de plataformas preservan mejor los datos y cuáles son más vulnerables? Según el profesor de ESIC, la banca electrónica y los grandes comercios *online* despuntan entre las plataformas más seguras. "Amazon, El Corte Inglés o Nike son seguros, pero hay comercios que todavía te redirigen a formularios para introducir tu número de tarjeta y eso no deberíamos hacerlo", apunta.

Todo lo contrario sucede con redes sociales como Facebook, Twitter o Instagram, que hacen del *big data* de sus usuarios "su negocio y en tanto en cuanto el servicio es gratuito, nuestros datos son el medio de pago", recalca. Maldonado, sin embargo, pone de relieve la importancia de las compañías de telecomunicaciones, que tienen acceso a toda la información personal introducida desde cualquier dispositivo móvil u ordenador: "La vulnerabilidad número uno está en las operadoras, que tienen acceso a todos los datos, incluidos los bancarios".