



Muchos expertos creen que los usuarios van a seguir sin leer la letra pequeña y sin detenerse a revisar los requisitos que propone la nueva legislación.

Nuestros datos, más seguros

El pasado 25 de mayo entró en vigor el nuevo Reglamento General sobre Protección de Datos, más conocido por sus siglas RGPD. El texto, aprobado por el Parlamento Europeo y la Comisión Europea en 2016, daba dos años de plazo a los Estados miembros de la UE para su adopción. Nuestros datos están hoy más seguros que hace unos meses, pero eso no quiere decir que debamos relajarnos ni dejar de asumir nuestra responsabilidad en este asunto.

MARIÁN LEZAUN

✉ marianlezaun@gmail.com

🐦 [@mlezaun](https://twitter.com/mlezaun)

PESE A QUE HAN TENIDO dos años para adaptarse a su contenido, la mayoría de empresas y organismos públicos han esperado al último momento para informar a los clientes y usuarios sobre la necesidad de dar una autorización expresa a la custodia de sus datos.

En las últimas semanas los buzones de correo han echado humo con la llegada de cientos de mensajes en los que se nos pedía consentimiento para guardar nuestros datos y se nos explicaba la nueva política de uso y protección de los mismos. Un cambio anunciado desde hace tiempo, pero que la mayoría de los consumidores han conocido recientemente y al que muchas pymes siguen sin adaptarse. La euforia y la preocupación apenas duraron unos días y pusieron de manifiesto lo vulnerable que es nuestra información una vez que decidimos compartirla.

Escaso impacto. Los expertos creen que, siendo optimistas, solo un 20% de esos correos se habrán respondido correctamente porque los usuarios van a seguir sin leer la letra pequeña y sin detenerse a revisar los requisitos que propone la nueva legislación. “Construir una política de

Beneficios del Reglamento

La puesta en marcha del reglamento ha traído importantes mejoras. Como explican los expertos, el beneficio más importante es, sin duda, el que no se ve porque nuestros datos van a estar más protegidos; la transferencia a terceros sin consentimiento no está permitida, y cualquier problema de seguridad que afecte a la privacidad de los usuarios debe de ser informado en un plazo de no más de 72 horas. Además, los datos no pueden guardarse más tiempo del necesario para la función que fueron recabados, aunque habrá que ver cómo se aplica esta cuestión en la realidad.

El segundo cambio está en la información que debe proporcionar quien recoge dichos datos: la finalidad, la duración, la legislación, etc. y todo ello debe ser presentado al usuario de forma clara, concisa, transparente y fácil de entender. Por otro lado los consentimientos deben ser explícitos e informados. Esto implicaría que la información sobre privacidad a los ciudadanos debe seguir mejorando.

En tercer lugar, mejora el derecho de acceso. Es decir, el derecho a obtener confirmación de la empresa u organización sobre si posee o no cualquier dato personal sobre una persona y en caso de tenerlo, el derecho a que le faciliten el acceso, una copia y a obtener toda la información adicional relevante (como el motivo del tratamiento de sus datos, las categorías de datos utilizadas, etc.).

Otro cambio importante hace referencia a la portabilidad de los datos: “si una empresa trata mis datos personales con mi consentimiento o basándose en un contrato, puedo pedirle que me los transfiera o los remita a otra empresa cuyos servicios quiero utilizar”, dice Subías.

También se podrá pedir que se borren nuestros datos personales cuando ya no sean necesarios o cuando hayan sido utilizados ilícitamente. Los datos personales que se facilitaron cuando alguien era menor pueden borrarse en cualquier momento. El procesamiento de datos personales de niños (menores de 16 años) solo será válido si lo autoriza el padre, la madre o un tutor legal.

El reglamento limita también la elaboración de perfiles y las decisiones automatizadas, práctica habitual en muchos sectores, como el bancario y financiero, el fiscal y la sanidad. La nueva norma estipula que tenemos derecho a no ser objeto de una decisión basada únicamente en medios automatizados, si la decisión produce efectos jurídicos en la persona o le afecta significativamente de modo similar.

Otro cambio importante es que las asociaciones pueden interponer reclamaciones, cosa que antes solo podían hacer los afectados. Además, las agencias de protección de datos dispondrán de un régimen sancionador mucho más potente que el actual ya que pueden imponer multas en función de la facturación de las empresas.

Para saber más



La Agencia Española de Protección de Datos ha puesto en marcha una herramienta gratuita para que cualquier empresa pueda desarrollar una correcta aplicación del nuevo reglamento.

► <http://cort.as/-7QKw>



La Asociación de Usuarios de Internet cuenta en su página con una guía para explicar cuáles son los nuevos derechos de los consumidores digitales.

► http://cort.as/-7Y_e



En ESCRITURA PÚBLICA hemos contado cuáles son los retos para los usuarios respecto al intercambio de datos.

► <http://cort.as/--6Ev>



protección de datos no es una tarea de las empresas: lo es de los ciudadanos y del sector público también. Me llama la atención no haber recibido noticias de alguna organización del sector público cuando se supone que son quienes deberían dar ejemplo”, lamenta Cecilia Álvarez, presidenta de la Asociación Profesional Española de Privacidad.

Y es que los usuarios debemos empezar a responsabilizarnos de nuestros datos personales. Cada vez que rellenamos un cuestionario, hacemos una compra *online*, nos registramos en cualquier empresa y compartimos información en las redes sociales, estamos perdiendo el control sobre nuestra información y debemos ser conscientes de esa situación. Pese al esfuerzo y las campañas realizadas, los expertos se muestran poco optimistas sobre lo informados que están los consumidores cuando entregan sus datos en cualquier soporte y con cualquier finalidad. “Es cierto que cada vez somos más conscientes de su importancia porque continuamente estamos viendo avances y cambios sociales derivados del binomio inteligencia artificial y datos personales, pero seguimos siendo igual de inconscientes en lo que respecta al riesgo que corre nuestra intimidad, derivado del uso de las

Cada vez que rellenamos un cuestionario, compramos *online* o nos registramos en cualquier empresa estamos perdiendo el control sobre nuestros datos



Los consumidores deben asumir una mayor responsabilidad en el uso de sus datos personales.



Los usuarios tienen derecho a que se eliminen sus datos en el momento en que ellos lo decidan

➔ nuevas tecnologías”, explica Miguel Pérez Subías, presidente de la Asociación de Usuarios de Internet. “El exceso de confianza nos hace ignorar las condiciones de uso y aceptar la cesión no solo de nuestros datos sino también de los de terceros ya que no tenemos ningún pudor en dar acceso a nuestra agenda de contactos, a nuestros álbumes de fotos o a diferentes servicios de geolocalización a quien nos lo pida siempre que sea, eso sí, a través de un móvil o un ordenador”, añade este experto.

Mayor preocupación. Más optimista se muestra Álvarez, quien considera que hay una mayor conciencia de la

importancia de la privacidad por una sucesión de casos que no han dejado indiferente a la opinión pública: brechas de seguridad muy importantes (en algunas autoridades públicas fiscales, entidades financieras, buscadores, redes sociales, etc.). “El escándalo de la compañía Cambridge Analytica, los casos de suplantación de identidad, el robo a una persona famosa que exponía su vida privada en redes sociales, la incipiente conciencia que tienen ya algunos usuarios de la conexión entre su comportamiento digital y los contenidos que recibe”, han servido para prestar mayor atención, según Álvarez. Para esta experta, resulta muy positivo que los

gigantes de internet, en aplicación de alguna sentencia de protección de datos y del Reglamento europeo, hayan modificado sus prácticas de privacidad poniendo a disposición de sus usuarios herramientas fáciles de utilizar de control de sus preferencias de privacidad.

En el mismo sentido, Víctor Domingo, presidente de la Asociación de Internautas, señala que la entrada en vigor del nuevo reglamento ha tenido un enorme impacto

En las últimas semanas se han enviado miles de mensajes en los que las empresas piden consentimiento ante la nueva política de protección de datos

mediático. “Ha servido para visualizar que la ingente cantidad de datos que circula por la Red a un ritmo viral se ha convertido en uno de los elementos más rentables para empresas y prestadores de servicios en internet.” “Otra cosa es que para muchos ciudadanos la defensa, el respeto a la privacidad de nuestros datos y la protección de los mismos por empresas e instituciones sigan siendo una asignatura pendiente”, reconoce Domingo. “De hecho cuando no valoramos lo suficiente nuestra privacidad y facilitamos información en exceso, estamos convirtiéndonos en meros productos gratuitos”, añade.

Por eso, el gran reto en el uso de los datos no es regulatorio sino ético y de competencia. “El principal problema al que nos enfrentamos es la falta de transparencia ya que no se dice todo lo que se hace con esa información y, además, se están creando auténticos monopolios o duopolios en la gestión de los datos personales y esto no es bueno para nadie”, apunta Subías. ●

Indemnizaciones y sanciones

SIN duda lo más llamativo del nuevo reglamento es la existencia de multas administrativas de hasta 20 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Es decir, el volumen de negocio será un factor relevante para la imposición de sanciones a aplicar. Los afectados por un tratamiento ilícito de datos personales podrán exigir indemnizaciones por daños y perjuicios y, aunque la norma recoge diferentes medidas para ver si las empresas están cumpliendo con sus obligaciones, serán los afectados los que deberán comunicar a la Agencia de Protección de Datos si creen que se están vulnerando sus derechos.



GUSTAVO SAMAYOA,
presidente FUCI (Federación
de Usuarios y Consumidores
Independientes)

✉ fuciest@hotmail.com

Los derechos de los usuarios ante el nuevo Reglamento de Protección de Datos

A PARTIR DE LA ENTRADA en vigor, el 25 de mayo de 2018, del Reglamento general de protección de datos de la Unión Europea, el usuario podrá controlar la información personal que ceden a cualquier empresa o servicio, y pedir compensaciones, si se incumple la norma.

Uno de los soportes de la norma es la transparencia en la utilización de los datos personales, mediante una información clara y veraz, que en ningún caso pueda llevar a equívoco al usuario.

Los datos protegidos son el nombre, las fotos, las direcciones de correo electrónico, los bancarios, las publicaciones en sitios web de redes sociales, la información médica o una dirección IP de un ordenador, entre otros.

La norma trae unos nuevos derechos para el usuario europeo, tanto frente a empresas o servicios que operen dentro de la UE, como aquellas que operen desde fuera.

El consentimiento expreso, es uno de los principales derechos que prevé la norma, en el sentido que el mismo ha de ser requerido por la otra parte, para el uso de sus datos y su finalidad. Este consentimiento ha de ser siempre por defecto, es decir, que es necesario que el usuario dé su autorización y no que se le induzca a ello a través de casillas pre marcadas con este consentimiento o que se indique que en caso de no responder se dará por contestado afirmativamente, es decir, el consentimiento tácito. Este consentimiento, dice la norma, ha de ser claro, inequívoco y distinguible de otros asuntos. Cuando un usuario se dé de alta en una web, servicio, aplicación o producto, el aceptar los términos del producto va por un lado y, por otro, todo lo relativo al tratamiento de datos. Por lo tanto, son ilegales casillas pre marcadas para el envío de publicidad, consentimientos tácitos para comunicaciones comerciales o cesiones de datos.

El usuario tiene que saber que ante los correos que viene recibiendo desde la entrada en vigor de la norma por parte de diferentes empresas para revalidar el permiso para mantener su información, tiene completa libertad para hacerlo o no mediante el mencionado consentimiento expreso. Si no lo revalida, y lo siguen utilizando, este registro es ilegal y por lo tanto cabe denunciar la situación ante la Agencia de Protección de Datos, organismo encargado de velar por la seguridad de los usuarios, mediante inspecciones y aplicación de las sanciones correspondientes. En caso de denuncia, será el denunciado el que habrá de probar que tenía los datos del usuario de forma lícita.

Otro de los derechos contemplados es el referido a la posibilidad de limitar el tiempo que los datos de los usuarios pueden ser guardados. El principio de minimización de la norma es importante de cara a que solamente sean tratados los datos imprescindibles y guardados para la finalidad propia para la cual se tratan, informando siempre del plazo de conservación de los mismos.

El usuario tiene derecho también a que sus datos sean eliminados cuando ya no sean necesarios para la finalidad con la que fueron recogidos; cuando se haya retirado el consentimiento, o cuando estos se hayan recogido de forma ilícita.

El derecho al olvido, que si bien no es un derecho absoluto, pues confronta con otros derechos como la libre información o con los datos de interés público, sí es un derecho que puede alegar el usuario, si bien sería necesario ponderarlo en cada caso según unos determinados criterios, que junto con la determinación de cuándo empieza la minoría de edad de un usuario o la portabilidad de los datos, serían temas a tratar y aclarar con la reforma inminente de la ley de protección de datos española.

El usuario también tendría derecho a portar sus datos, es decir a cederlos a otro servicio o empresa, siempre y cuando se trate de aquellos que el usuario haya cedido y no aquellos que haya ido dejando con sus acciones en la red social.

Y por último el usuario tiene el derecho de acceso, es decir que podrá pedir que confirmen si sus datos se están procesando, en dónde y con qué fin. Se podrá pedir una copia de los datos personales en formato electrónico y de forma gratuita.

Como conclusión, podemos decir que el usuario cuenta con más derechos, pero ha de ser este de forma responsable, el que utilice las nuevas tecnologías con las debidas precauciones y que no olvide que también existen unas obligaciones por su parte.

«Son ilegales casillas pre marcadas para el envío de publicidad, consentimientos tácitos para comunicaciones comerciales o cesiones de datos»

**“Por una Ley
contra la
Obsolescencia
Programada
en España”**

