EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS NO ES UNA AMENAZA, SINO UNA OPORTUNIDAD

EN BREVE

Si somos capaces de mirar a medio o largo plazo, podremos identificar que el Reglamento General de Protección de datos, a punto de cumplir un año de inicio de aplicación en Europa, es una oportunidad de poner orden al mundo digital, y lograr trasladar todos los derechos fundamentales que hasta ahora hemos ido conquistando como sociedad, en concreto el derecho fundamental a la intimidad y privacidad de las personas, al ecosistema online para seguir generando una convivencia pacífica y prosperidad.

En este sentido, el RGPD no pretende ser un *stopper*, sino una herramienta fundamental para que todos aquellos que traten datos personales (responsables y encargados principalmente) cumplan con la protección de datos en función de sus capacidades y uso efectivo de los datos, evitando imponer la misma carga de obligaciones a situaciones radicalmente diferentes, en la búsqueda de una cultura de cumplimiento generalizado que garantice a todos las personas un nivel de compromiso por parte de aquellas empresas cuyo negocio, eficiencia y explotación económica se basa en los datos personales -las *data driven companies*-.

SUMARIO

MIGUEL ORTEGO RUIZ

ABOGADO Y PROFESOR EN DERECHO.SOCIO FUNDADOR DE MEDIALAW ABOGADOS. CIPP/E

NOVEDADES FUNDAMENTALES DEL RGPD Y LA LOPDGDD

El 25 de mayo de 2018 comenzó a aplicarse en todos los Estados miembros de la Unión Europea (en adelante, UE) el Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (en adelante, RGPD), y el pasado 7 de diciembre de 2018 hacía lo propio la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD). Desde entonces está en marcha, el conjunto al que podemos denominar la **nueva Normativa de Protección de Datos Personales**, y regula una cuestión

LEGISLACIÓN www.globaleconomistjurist.com

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (Legislación. Marginal: 70341505). Arts.; 2.2.c), 4.1, Considerando núm. 26º

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (Legislación. Marginal: 70852038). Arts.; 6, 9, 10, 85, 86

no menor como es el derecho fundamental a la intimidad y privacidad personales. Y todavía está por llegar un Reglamento en materia de cookies (el denominado Reglamento *ePrivacy*) que sustituya a la actual Directiva *ePrivacy*[1], aunque parece que su entrada en escena se hará esperar.[2]

A pesar de que los cambios introducidos -por el RGPD fundamentalmente- respecto de la normativa española de protección de datos clásica -la LOPD y su Reglamento de desarrollo- son cuantiosos, y algunos de ellos bastante revolucionarios, **muchas cuestiones se han clarificado y simplificado en pro de un sistema más flexible y adaptable a la realidad económica actual**, que fundamentalmente se basa en lo digital -y es ahí donde los datos son la piedra angular de todo el sistema-.

El RGPD ha supuesto que desaparezca el rígido y burocrático sistema de comunicación

> "DESDE DICIEMBRE DE 2018 ESTÁ EN MARCHA Y A PLENO RENDIMIENTO TODA LA NORMATIVA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES"

1 Y que no solo regulará las cookies, sino también las direcciones MAC, los números IMEI de los Smartphone, etc., Vid., Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) COM (2017) 10 final, 2017/0003 (COD).

2 *Las elecciones al Parlamento Europeo de mayo de 2019 van a retrasar la publicación del Reglamento ePrivacy (prevista para este año) lo que supone que, contando con el periodo de carencia de aplicación (generalmente de 24 meses, como ya ocurrió con el RGPD), el Reglamento ePrivacy sea de aplicación para el 2021.*

JURISPRUDENCIA www.globaleconomistjurist.com

– Sentencia del Tribunal Supremo de fecha 3 de octubre de 2014, núm. 3896/2014, Nº Rec. 6153/2011 (Marginal: 69526249)

– Sentencia del Tribunal de Justicia de la Unión Europea de fecha 19 de octubre de 2016, asunto C-582/14 Pratrick Breyer (Marginal: 70339861)

y alta de los ficheros ante la Agencia Española de Protección de Datos (en adelante, AEPD), o el encorsetado procedimiento de niveles y medidas de seguridad de los datos en función de su tipología -de nivel básico, medio y alto-.

La novedad de **la nueva Normativa de Protección de Datos Personales busca ser más flexible y adaptativa**, ya que aborda el sistema de protección de datos personales de tal forma que los obligados a cumplirla lo puedan hacer en función del caso particular, de los datos, fines y tratamientos que realicen.

La LOPDGDD, por su parte, **básicamente se dedica a regular por remisión al articulado del RGPD la mayoría de las cuestiones**, como no podía ser de otra manera, dado que el RGPD es de aplicación directa en todos los Estados miembros y no necesita del mecanismo clásico de las Directivas europeas de la transposición al Derecho interno. **Pero**, además, **ha introducido alguna que otra novedad** como la regulación del derecho a la protección de datos de los fallecidos, los derechos de rectificación y actualización de informaciones en los medios de comunicación digitales,[3] o los inéditos hasta ahora en nuestro Ordenamiento Jurídico "derechos digitales" y sus garantías -un conjunto de *desiderata* en relación a éstos más que una regulación propiamente dicha, pero por algo se empieza-.

Junto con las clásicas figuras del **responsable del tratamiento** -aquél que decide cuáles son los fines y medios del tratamiento-, **el encargado del tratamiento** -aquél que trata los datos por cuenta, encargo, del responsable- y el **interesado** -cualquier persona física identificada o identificable cuyos datos se tratan-; el RGPD ha introducido una figura que si bien no es inédita, sí que es la primera vez que se incorpora expresamente a la regulación de obligado cumplimiento en Europa: **el Delegado de Protección de Datos o *Data Protection Officer*** (en adelante, DPO). El DPO básicamente es un experto en la materia **cuya misión es ayudar a los responsables y encargados a cumplir la Normativa de Protección de Datos Personales**.

El DPO es voluntario para todos aquellos que quieran contratar uno -pudiendo incluso un mismo DPO actuar como tal para varios

3 *Vid., arts. 85 y 86 de la LOPDGDD.*

responsables y/o encargados- y una **figura obligatoria para los responsables en ciertos casos**, esto es, (1) cuando el tratamiento de datos lo realice una Autoridad u Organismo Público; (2) cuando se realice un tratamiento a gran escala de los denominados datos sensibles y sobre condenas penales; (3) cuando el tratamiento consista en una observación habitual y sistemática de interesados a gran escala; o (4) si una Ley de un Estado miembro así lo exige.

Otra de las novedades fundamentales del RGPD son las denominadas **Evaluaciones de Impacto de Protección de Datos** (en adelante, EIPD) y que responden al cambio de enfoque que ha implicado la nueva Normativa de Protección de Datos. En resumidas cuentas, ahora **los responsables y encargados deben conocer** a ciencia cierta **qué datos y qué tratamientos de los mismos realizan, y determinar el riesgo asociado a todo ello**, esto es, deben realizar un **mapa de riesgos** (*risks assessment* en inglés) sobre el cual se fundamentará toda su política y obligaciones de privacidad y protección de datos.

Las EIPD son voluntarias -aunque muy recomendables en todo caso- y, bajo ciertas circunstancias, el responsable o encargado está obligado a afrontarla de manera obligatoria; esto es: (1) cuando se realice una evaluación sistemática y exhaustiva de los interesados que se base en un tratamiento automatizado que sirva de base para tomar decisiones (lo que en marketing digital se denomina "perfilado" o elaboración de perfiles de usuarios); (2) cuando se realicen tratamientos a gran escala de datos sensibles o sobre condenas penales; (3) cuando se lleve a cabo una observación sistematizada a gran escala de una zona de acceso público; y (4) cuando así lo determine expresamente la AEPD, pudiendo añadir o modificar este listado según lo vaya considerando oportuno.

Por último, y en lo que a este breve repaso general de algunas de las novedades del RGPD respecta, éste **ha introducido** esencialmente el denominado **principio de responsabilidad proactiva** o *accountability*, cuyo fin primordial es que la actitud de los responsables y encargados -y de la sociedad en general- no sea meramente defensiva, generando un cierto rechazo hacia la materia, sino proactiva y basada en la iniciativa por cumplir una Normativa de Protección de Datos que a la postre lo que nos está haciendo es una colectividad más respetuosa para con uno de los pilares del Estado Social y Democrático de Derecho -también a un nivel europeo, de la UE-. En muy poco tiempo, la regulación de protección de datos será tan común y corriente para todos, como lo es hoy en día el sistema tributario o mercantil, por ejemplo, que lo raro será no pensar en las **implicaciones que cualquier actividad económica tiene en la privacidad y los datos de los individuos**. De hecho, nadie concibe hoy que alguien entre en tu casa sin tener permiso, o te grabe en la intimidad de tu salón sin tu permiso y se lucre con ese contenido, pues son pilares nucleares de nuestra sociedad; ¿por qué nos parece tan raro que queramos regular conductas análogas en el mundo digital, que, lógicamente, conlleva realizar ciertos comportamientos?

"EN MUY POCO TIEMPO, LA REGULACIÓN DE PROTECCIÓN DE DATOS SERÁ TAN COMÚN Y CORRIENTE PARA TODOS, QUE LO RARO SERÁ NO PENSAR EN LAS IMPLICACIONES QUE CUALQUIER ACTIVIDAD ECONÓMICA TIENE EN LA PRIVACIDAD Y LOS DATOS DE LOS INDIVIDUOS"

Como partes esenciales de la *accountability* destacan los principios de "**privacidad por defecto**" y "**privacidad en el diseño**" y que pocas palabras consisten en la obligación de todo responsable de valorar -con DPO si es posible- qué implicaciones -impacto fundamentalmente- puede tener un nuevo producto o servicio en la privacidad e intimidad de los ciudadanos a los que se dirige; en sus datos personales. Esta evolución, que debe de hacerse desde el punto de vista de los riesgos, debe quedar registrada de alguna forma por si fuera pertinente en algún momento.

> "CUANDO NOS FIJAMOS EN LAS SANCIONES, HASTA 10 O 20 MILLONES DE EUROS, INCLUSO MÁS PARA LAS EMPRESAS, PENSAMOS QUE QUIZÁ SON EXAGERADAS, PERO ¿CUÁNTO VALE NUESTRA PRIVACIDAD E INTIMIDAD"

Las **sanciones administrativas** (que no impiden indemnizaciones civiles añadidas) **también se han visto modificadas** -considerablemente- **por el RGPD**. Hasta 2018, en España, la sanción máxima, para infracciones muy graves, era de 600.000 €; ahora, con el RGPD, las sanciones llegan hasta los diez millones de euros, o **hasta veinte millones de euros** (las más graves), sin perjuicio de que las empresas puedan verse involucradas en multas muy superiores a esas cifras.

¿CUÁNDO Y CÓMO APLICAR EL RGPD?

Al principio, como es normal, **los cambios son tan disruptivos** -como lo es la tecnología que hay detrás de estas modificaciones sociales, económicas y jurídicas (y por este orden)- **que se generan unas fuertes resistencias a aplicar y entender las novedades normativas de la nueva realidad**. Esto impide que cueste más entender normas como el RGPD. Y cuando algo no se entiende -quizá porque no se explica "bien"- no se genera otra cosa que rechazo. Esto es lo que ocurre con el RGPD (además de los costes y complejidades técnicas asociados) que dificultan su implementación. Al final todo queda en un puñado de dificultados y gastos a corto plazo pero que, a medio o largo plazo, son "árboles que nos impiden ver el bosque".

El punto de partida -y lo fundamental- en relación con la Normativa de Protección de Datos Personales **es determinar cuándo nos encontramos con datos personales** (y, por tanto, debemos cumplir con la Normativa de Protección de Datos), **y cuándo no**. A pesar de que **el RGPD ha ampliado el concepto de datos personales**, incluyendo cuestiones novedosas como los datos biométricos o los datos genéticos, lo cierto es que los cimientos no han cambiado, y la base para determinar si nos encontramos ante datos personales, o no, sigue siendo que se trate de una "**información sobre una persona física identificada o identificable**[4]", esto es, que no siendo identificable -a priori- se pueda identificar indirectamente -cruzando datos por ejemplo- por medios razonables[5] y efectivos.

De esta manera, **los datos anónimos o anonimizados** -sin posibilidad de reversión-

4 *Vid., art. 4.1 del RGPD.*
5 *Vid., Considerando número 26º del RGPD.*

y los datos de las personas jurídicas no son datos personales a efectos del RGPD. Tampoco los tratamientos de datos personales efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas[6].

Una de las cuestiones más complejas y relevantes en la imbricación del RGPD y la economía digital es la determinación de **si las direcciones IP o los identificadores en línea** (un "ID", como por ejemplo los de un navegador de Internet) son, o no datos personales a los efectos de la Normativa de Protección de Datos. La clave está, como hemos expuesto más arriba, en si permiten identificar -directa o indirectamente- a una persona física.

Para algunos expertos en tecnología una dirección IP o un ID, así, en "bruto" (sin registro de usuario), **no permiten identificar a la persona física**, toda vez que para ello habría que requerir al proveedor de servicios de Internet de turno que aportara estos datos, y esto sólo cabe en nuestro Ordenamiento Jurídico por orden de un Juez o Tribunal. **La Agencia Española de Protección de Datos** -ya antes incluso de la llegada del RGPD-[7], **el Tribunal Supremo** (TS)[8] **y el Tribunal de Justicia de la Unión Europea** (TJUE[9]) e**ntienden que las direcciones IP** -estáticas o dinámicas- **son datos personales**. Algo que puede ser complicado de entender desde el punto de vista estrictamente técnico, pues parece que no casa muy bien con esa necesidad de identificar a la persona física a través de medios razonables -en el sentido de que no supongan un esfuerzo y costes desmedidos-. En cualquier caso, es ésta una cuestión lo suficientemente compleja para que podamos abordarla en este momento.

Sea como fuere, en lo que a nosotros nos interesa ahora, **los datos personales** -los denominados sensibles del artículo 9 y los referidos a condenas penales del artículo 10 requieren además un plus- **pueden ser tratados si se cumple una -o varias- de las denominadas bases de licitud** del RGPD (art. 6), y que son: (1) contar con el consentimiento del interesado (debe ser expreso, y el responsable ha de ser capaz de demostrar que lo obtuvo); (2) que necesitemos tratar los datos para ejecutar un contrato (por ejemplo las datos personales de los firmantes del contrato);

> "TODO CAMBIO IMPLICA UNAS RESISTENCIAS QUE A CORTO PLAZO PUEDEN SER COMPRENSIBLES, PERO QUE A MEDIO O LARGO PLAZO SON LOS ÁRBOLES QUE NOS IMPIDEN VER EL BOSQUE"

6 *Vid., art. 2.2.c) del RGPD.*
7 *Cfr., Informe 327/2003*
8 *Vid., STS (Sala 3ª) número 3896/2014 de 3 de octubre de 2014 (RJ 6153/2011), FJº 4º*
9 *Vid., STJUE (Sala 2ª) de 19 de octubre de 2016, asunto Pratrick Breyer (C-582/14), aptdo. 49º*

> "EN LA ECONOMÍA DIGITAL, CUANDO UN PRODUCTO O SERVICIO ES GRATIS, ENTONCES EL PRODUCTO O SERVICIO ERES TÚ: TUS DATOS PERSONALES"

(3) que el tratamiento sea necesario para cumplir una obligación legal impuesta al responsable (por ejemplo comunicar el salario bruto a la Hacienda Pública, y practicar la retención a efectos del IRPF que corresponda); (4) que necesitemos tratar los datos para proteger intereses vitales del interesado (en un accidente, llega una persona inconsciente y las asistencias le identifican por su D.N.I. y le trasladan la información al hospital que van de camino); (5) para el cumplimento de una misión en interés público o ejercicio

BIBLIOGRAFÍA www.globaleconomistjurist.com

BIBLIOTECA

– ORTEGA GIMÉNEZ, ALFONSO. Guía práctica sobre protección de datos de carácter personal para abogados. Ed. Difusión Jurídica. Madrid 2008.

ARTÍCULOS JURÍDICOS

– VILLASANTE, CRISTINA. *Identity manager: la importancia de gestionar la identidad online en la economía digital.* Abril 2019. Economist&Juris Nº 229 (www.economistjurist.es)

– ÉCIJA, ÁLVARO. *La ciberseguridad en los despachos de abogados*. Febrero 2019. Economist&Jurist Nº 227 (www.economistjurist.es)

– DIVÍ, MARÍA. *¿Qué tienen que tener en cuenta los despachos de abogados ante la entrada en vigor del Nuevo Reglamento de Protección de Datos?* Junio 2018. Economist&Jurist Nº 221 (www.economistjurist.es)

– DE MIGUEL, JAVIER. *Funciones y responsabilidades del delegado de protección de datos.* Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

– ORTEGA GIMÉNEZ, ALFONSO y GONZALO DOMENECH, JUAN JOSÉ. *Las transferencias internacionales de datos de carácter personal en el nuevo reglamento general de protección de datos*. Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

– MUÑOZ CORRAL, ERNESTO JOSÉ. *Las sanciones en caso de incumplimiento del reglamento general de protección de datos europeo*. Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

– MUÑOZ, JOAQUÍN. *Principios de protección de datos: Licitud, lealtad, transparencia, minimización, exactitud, integridad y confidencialidad*. Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

– ORTEGA GIMÉNEZ, ALFONSO. *Cuestiones de derecho internacional privado (competencia judicial internacional y determinación de la ley aplicable) en el nuevo reglamento general de protección de datos*. Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

– MARIMÓN PRATS, LUIS. *Derechos de las personas interesadas: acceso, rectificación, supresión, limitación del tratamiento, de portabilidad y de oposición*. Febrero 2018. Economist&Jurist Nº 217 (www.economistjurist.es)

de poderes públicos; y (6) el tratamiento es necesario para satisfacer los intereses legítimos del responsable, o un tercero (por ejemplo, para enviar información sobre nuevos productos a un cliente con el que has contratado antes para productos similares).

Finalmente, **el RGPD ha introducido nuevos derechos**, además de los clásicos "derechos ARCO" -acceso, rectificación, cancelación y oposición- entre los que destacan el derecho a no ser objeto de decisiones automatizadas basadas en el perfilado, **el derecho al olvido** -que no indexen los motores de búsqueda una noticia, no que ésta desaparezca-, **y el derecho a la portabilidad de los datos** -si fueron recogidos y tratado en forma electrónica y automatizada-.

CONCLUSIONES

- En la economía digital actual debemos de ser conscientes de que cuando algo es gratis es porque el producto somos nosotros, en concreto nuestros datos personales. Y estos tienen no solo un valor económico incalculable (se los denomina el "petróleo del siglo XXI"), sino que representan un derecho tan fundamental como la vida o la libertad, el derecho a la intimidad y privacidad de las personas.
- La tecnología está produciendo una disrupción social y económica que, como no podía ser de otra forma, se traslada también al ámbito jurídico, y los cambios son tan relevantes que la aplicación de normas como el RGPD generan unas reticencias y resistencias hasta cierto punto lógicas.
- Sin embargo, no podemos dejar que el posicionamiento defensivo frente al cambio nos impida ver cuán importante es que entendamos y cumplamos (o viceversa) normas que regulan derechos fundamentales como el RGPD. Con el tiempo toda la Normativa de Protección de Datos será tan común, y estará tan interiorizada en nuestra sociedad como lo están hoy en día otras como la fiscalidad o el sistema hipotecario; entre tanto, nuestra contribución debe ser aceptar el cambio y ayudar a que ocurra lo más pacíficamente posible, y para ello cuanto más formados estemos en materia de protección de datos personales y más conozcamos la normativa, como el RGPD, por ejemplo, mejor. En este sentido los docentes también tenemos una responsabilidad a la hora de emplear nuestros mejores esfuerzos en trasladar esta materia a la sociedad de una forma lo más didáctica posible, pues, a la larga, todos lo agradeceremos.