Ars Iuris Salmanticensis
TRIBUNA DE ACTUALIDAD
Vol. 6, 11-16
Junio 2018
eISSN: 2340-5155

El Reglamento General de Protección de Datos, un mes después de su aplicación

The General Data Protection Regulation, one month after its application

Enrique NIETO MANIBARDO
Abogado Despacho NIVOLAP

Fecha de recepción: 19 de junio de 2018

Fecha de aceptación definitiva: 20 de junio de 2018

Todas las organizaciones han oído hablar de la nueva normativa de protección de datos, el Reglamento (UE) General de Protección de Datos (RGPD o GDPR por sus siglas en inglés); casi todos saben que cambia radicalmente la forma de tratar los datos para las empresas, autónomos y Administraciones públicas; algunos saben las novedades que trae consigo esta nueva norma europea; pero muy pocos han hecho los deberes llegado el día en que se empezó a aplicar, el 25 de mayo de 2018.

Están obligados a cumplir el RGPD todas las empresas, Administraciones públicas, asociaciones, fundaciones, etc., que traten datos de carácter personal de personas físicas[1]. Por el contrario, los particulares no se ven sometidos a esta regulación[2]. Pero ello no significa que todos nosotros, como particulares, nos despreocupemos sobre la

1. Artículo 1.1 en relación con el artículo 4, apartado 1, ambos del Reglamento (UE) General de Protección de Datos.
2. Artículo 2.2,c) del Reglamento General de Protección de Datos.

protección de nuestros datos de carácter personal, puesto que la finalidad del RGPD es aportar un nivel mucho mayor de protección de tus datos, a la par que aumenta los derechos de los ciudadanos. ¿Quién no tiene descargada en su smartphone una app? ¿Quién no tiene que ir al médico y le piden sus datos (incluida la enfermedad y el historial clínico)? ¿Quién no utiliza redes sociales? ¿Quién no ha cedido sus datos a la Universidad? ¿Quién no da sus datos a la empresa en la que trabaja? O, simplemente, ¿quién no cede su nombre y apellidos para que le puedan facturar un producto o servicio?

Cuando realizamos cualquier acto de este tipo, debemos saber que afecta a un derecho fundamental autónomo, el derecho a la protección de datos (artículo 18.4 de la Constitución española), también denominado «autodeterminación informativa» o (como prefiere denominarlo el Tribunal Constitucional) «libertad informática»[3].

Un derecho en auge, que se ha convertido en la moneda de cambio para disfrutar «gratuitamente» de servicios; un derecho del que ha surgido una nueva economía basada en el tratamiento de datos; un derecho, en fin, que tiene una repercusión exacerbada sobre nuestra privacidad. Muchas empresas (sobre todo las más grandes, pensemos en Google, Facebook, Amazon o Apple) saben de nosotros más que nuestros amigos, nuestra familia, nuestra pareja o, incluso, en muchas ocasiones, más que nosotros mismos.

Advierte SANTAMARÍA RAMOS sobre los peligros futuros de los datos y su tratamiento ulterior, señalando que «El dato se ha convertido en la unidad básica de la sociedad de la información, y por tanto cualquier organización se encuentra en la necesidad de recolectar datos de carácter personal como forma de maximizar sus beneficios»[4].

Todo ello exige concienciación sobre todo lo que implica el tratamiento masivo de datos, y ello conlleva que debemos ser plenamente conscientes de esta nueva norma europea. Sí, las empresas son las obligadas a adaptarse al nuevo modelo, pero todos

3. Las SSTC 292/2000, de 30 de noviembre, y 96/2012, de 7 de mayo, establecen que el derecho a la protección de datos se concreta en «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión de uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder de oponerse a esa posesión y usos».

4. SANTAMARÍA RAMOS, F. J. 2011: *El encargado independiente. Figura clave para un nuevo Derecho de protección de datos.* Madrid: La Ley grupo Wolters Kluwer, 512-513.

somos responsables de exigir que se traten nuestros datos con garantías y acorde a la ley.

Afortunadamente, el interés de los españoles sigue creciendo en torno a su derecho a la protección de datos de carácter personal, y eso, en mi opinión, es un aliciente para que las empresas cumplan con el RGPD. Al final, las que cumplan con todos los derechos y garantías de los particulares gozarán de una ventaja competitiva y darán una imagen mucho más positiva que aquellas que no lo hagan.

Ante esta situación, me planteo si estamos listos para aplicar con garantías el RGPD un mes después del 25 de mayo y qué está ocurriendo en España por parte de todos los agentes implicados en el cumplimiento de la normativa sobre protección de datos.

Pues bien, la realidad es que existe un retraso generalizado de todas las partes intervinientes, desde el legislador al último autónomo, pasando por Administraciones públicas y empresas.

Recordemos que el RGPD lleva dos años en vigor, y es este plazo el concedido a los Estados miembro para que se adapten. Queda atrás el 25 de mayo y falta mucho aún por hacer.

En primer lugar, la entrada en vigor del RGPD exige una nueva norma española, una nueva Ley Orgánica de Protección de Datos (LOPD) que se ajuste a los postulados del RGPD. Entretanto no haya nueva Ley, se seguirá aplicando la antigua (y vigente LOPD) y el Reglamento que desarrolla la misma en todo aquello que no contravenga a la nueva norma europea. Hasta aquí bien, pero ¿qué ocurre con aquello en que la ley española se oponga a la europea? No cabe duda de que el RGPD es de aplicación, desplazando a la LOPD. Pero hay casos en que no es fácil entrelazar ambas normas, por ejemplo, en relación a las sanciones o menores de edad, en los cuales el RGPD da libertad a los Estados miembro para que concreten dentro de los márgenes fijados.

En cuanto a las sanciones, nos encontramos ante una difícil labor de conjugar ambas normas. Por un lado, la LOPD establece tres tramos de infracción: leve, grave y muy grave, a cada uno de los cuales se le asigna un rango de sanciones diferente, siendo la mínima de 900 euros y la máxima sanción de 600.000 euros[5]. El RGPD, por el contrario, no establece una cuantía mínima, sino únicamente estipula la posibilidad de sancionar con multas de hasta 10.000.000 o 20.000.000 euros o, tratándose de una empresa, de una cuantía equivalente al 2% o el 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía[6]. Entonces, ¿cómo va la AEPD a imponer sanciones sin un parámetro claro al que adherirse? Antes de aplicarse el RGPD, por tanto, necesitamos una Ley española que concrete los sujetos responsables, los plazos de prescripción y las cuantías.

5. Artículo 45 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

6. Artículo 83, apartados 4, 5 y 6 del Reglamento (UE) 2016/679, General de Protección de Datos.

Ars Iuris Salmanticensis,
vol. 6, Junio 2018, 11-16
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

Además, con relación a los menores de edad es necesario que se recoja igualmente en la Ley Orgánica de Protección de Datos cuál va a ser la edad mínima para que un menor pueda consentir el tratamiento de sus datos personales. El RGPD señala que a partir de los 16 años, pero da libertad a los Estados para que fijen una edad inferior, con el límite de los 13 años[7]. Esto es, España podría recoger en la nueva Ley que los menores pueden consentir el tratamiento de sus datos en una edad comprendida entre los 13 y los 16 años. De acuerdo con el Reglamento de desarrollo de la LOPD esa edad se fija en los 14 años[8], pero parece que en la nueva Ley se pretende fijar en los 13 años[9]. En fin, existe una incertidumbre para todas las empresas e instituciones que deben actualizar sus políticas de privacidad. Algunas de ellas han optado por establecer una edad mínima para consentir de 16 años, en consonancia con el RGPD y dejando de lado una nueva Ley española que debería estar, a estas alturas, ya lista para aplicarse.

Podía parecer que este retraso del legislador llevaba implícita una prórroga o un periodo «extra» pretendido para adaptarse al RGPD, sin embargo, el RGPD fue aplicable a partir del 25 de mayo en todos los Estados pertenecientes a la UE y, en palabras de Mar España (directora de la AEPD), en una entrevista concedida para «elpais»[10], a escasos días de la fecha de aplicación de la nueva normativa, señaló claramente lo que vino repitiendo a lo largo de los últimos meses: no existiría tal prórroga.

Ciertamente, sin la nueva Ley, todos los ciudadanos que quieran ejercer sus derechos, las empresas obligadas a garantizarlos y los profesionales que trabajamos en el asesoramiento de unos y otros nos vemos sumergidos en un escenario complicado, en una ardua tarea de entretejer el RGPD y la actual LOPD.

Si, teniendo presente la importancia, como se ha visto, de la aprobación de una nueva LOPD, no se actúa a tiempo por legislador, no es de extrañar que la empresa española no esté lista, en términos generales, llegado el día de aplicar el RGPD.

En un estudio que se hizo tres meses antes del 25 de mayo, denominado «Cómo acelerar el cumplimiento del GDPR»[11], elaborado por International Data Corporation (IDC) y Microsoft, aunque carece de valor estadístico, puesto que son consultadas 100 empresas de más de 250 empleados, permite hacernos una idea del desconocimiento y falta de precauciones de muchas empresas.

7. Artículo 8 del Reglamento (UE) 2016/679, General de Protección de Datos.

8. Artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

9. Artículo 7 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (24 de noviembre de 2017).

10. https://cincodias.elpais.com/cincodias/2018/05/10/companias/1525982295_623174.html?id_externo_rsoc=FB_CC.

11. https://news.microsoft.com/uploads/2018/02/IDC-MSFT-Como-acelerar-cumplimiento-GDPR.pdf.

El estudio muestra que solo el 10% de las empresas cumplen el RGPD, el 25% tiene un plan sólido para asegurar el cumplimiento a la fecha de aplicación, el 35% tenía pensado arrancar en 2017, el 15% se encuentra a la espera de más información y el 5% no sabe por dónde empezar.

No obstante, este estudio se realizó en enero de 2018, por lo que presumo que desde entonces muchas empresas han tomado medidas. Pero hay que tener en cuenta que las empresas consultadas, como dije, tienen más de 250 trabajadores, es decir, empresas que presumiblemente tendrán capacidad económica para actuar. Lo que quiere decir que en las pequeñas y medianas empresas y los autónomos los porcentajes de desconocimiento, desinformación y falta de previsión probablemente sean mucho mayores.

La mayor preocupación de las empresas, incluso más que las multas, es la pérdida reputacional, el daño que puede ocasionar a la reputación de la empresa una violación de la información, puesto que el 80% de los ciudadanos que vean vulnerada su información personal no volverán a confiar nunca en esa empresa.

Para evitar el incumplimiento del RGPD, esta misma norma prevé una nueva figura, el DPD (Delegado de Protección de Datos), que será el encargado de coordinar toda la adaptación, supervisar el cumplimiento, cooperar con las autoridades de control, etc. Esta figura es obligatoria para las Administraciones públicas y para algunas empresas, no para todas, pero, en cualquier caso, cada empresa puede decidir voluntariamente nombrar un DPD.

Pues bien, tampoco hay buenas noticias respecto al cumplimiento del deber de nombrar Delegados de Protección de Datos, puesto que, en palabras de la directora de la AEPD[12], solo ha habido 1.300 notificaciones de nombramientos de DPD. De ellas, casi 1.000 pertenecen al sector privado, por lo que el sector público solo ha procedido de momento a poco más de 300 notificaciones. Recordemos que para las Administraciones públicas es obligatorio nombrar un DPD (excepto los Tribunales)[13], y en España hay unos 20.000 organismos públicos.

Y a propósito de ello, hay una falta de concreción sobre la obligatoriedad del DPD en las organizaciones, puesto que el RGPD contiene «zonas oscuras» que hacen difícil vislumbrar en algunos casos si es necesario proceder al nombramiento de esta figura o no. Al respecto se ha pronunciado el Grupo de Trabajo del artículo 29, que intenta abordar estas dificultades de interpretación[14], pero, a mi juicio, no es suficiente, siendo

12. https://cincodias.elpais.com/cincodias/2018/05/10/companias/1525982295_623174.html?id_externo_rsoc=FB_CC.

13. Artículo 37.1, apartado a) del Reglamento (UE) 2016/679, General de Protección de Datos.

14. Ver «Directrices sobre los Delegados de Protección de Datos (DPD)», adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017, Grupo de Trabajo sobre Protección de Datos del artículo 29.

necesario contar con una ley estatal que concrete los supuestos y las organizaciones que tienen obligación de nombrar un DPD.

En conclusión, los dos años que Europa concedió a los Estados miembro para que, paulatinamente, fuesen adoptando sus políticas, procedimientos, etc., al nuevo RGPD, en términos generales, parece que no han sido aprovechados ni por las empresas ni por las administraciones públicas y, lo que tiene más demérito, por el legislador.

La añorada, por algunos, prórroga o periodo «extra» parecía que no iba a ser posible y, efectivamente, así ha sido.

Ante ello, me surge la duda de si las empresas españolas son conscientes de la importancia en el cumplimiento de la normativa de protección de datos, o si, por el contrario, piensan que es algo transitorio. La adaptación a la nueva normativa, desde luego, solo es el principio, en mi opinión, de una nueva forma de tratar los datos personales, de un cambio en la mentalidad de todos los entes que intervengan en el tratamiento de los datos y de todos los ciudadanos titulares de los datos personales que se tratan. Si es así, pienso firmemente que es mejor cumplir desde un primer momento y no esperar a que lleguen las multas o la pérdida de reputación y de imagen de la empresa.

En cuanto a las Administraciones públicas y poderes del Estado, tratándose de un derecho fundamental tan importante en la economía digital en la que nos encontramos inmersos, me parece sorprendente (o quizás no tanto) que actúen con esta falta de diligencia y previsión. No perdamos de vista la función de las Administraciones y poderes públicos, que no es otra que velar por los derechos de las personas.

Ars Iuris Salmanticensis,
vol. 6, Junio 2018, 11-16
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND