Decálogo sobre a nova normativa de protección de datos

Decálogo sobre la nueva normativa de protección de datos

Decalogue on the new data protection regulations

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ
Profesor titular de Derecho Constitucional
Delegado de Protección de Datos
Universidad de Santiago de Compostela
josejul.fernandez@usc.es

Recibido: 15/11/2018 | 22/01/2019

Resumo: O artigo aborda os dez aspectos máis relevantes da nova normativa de protección de datos, sobre a base do Regulamento UE 2016/679 e a Lei orgánica 3/2018. Iso faise tanto desde un punto de vista descritivo como desde posicións máis analíticas e explicativas. Previamente faise un enfoque situacional que subliña o papel que representa na actualidade o dereito fundamental á protección de datos no marco dunha Sociedade da Información hiperglobalizada. O enfoque, aínda que resulta preferentemente xurídico, complétase con aspectos sociolóxicos e politolóxicos.
Palabras clave: Protección de datos, Regulamento (UE) 2016/679, LO 3/2018, dereito fundamental, principios, bases de lexitimación, dereitos, responsable de tratamento, delegado de protección de datos, autoridade de protección de datos, infraccións e sancións.

Resumen: El artículo aborda los diez aspectos más relevantes de la nueva normativa de protección de datos, sobre la base del Reglamento UE 2016/679 y la Ley orgánica 3/2018. Ello se hace tanto desde un punto de vista descriptivo como desde posiciones más analíticas y explicativas. Previamente se realiza un enfoque situacional que subraya el papel que representa en la actualidad el derecho fundamental a la protección de datos en el marco de una Sociedad de la Información hiperglobalizada. El enfoque, aunque resulta preferentemente jurídico, se completa con aspectos sociológicos y politológicos.
Palabras clave: Protección de datos, Reglamento (UE) 2016/679, LO 3/2018, derecho fundamental, principios, bases de legitimación, derechos, responsable de tratamiento, delegado de protección de datos, autoridad de protección de datos, infracciones y sanciones.

Abstract: The paper addresses the ten most relevant aspects of the new data protection regulations, based on the Regulation EU 2016/679 and Organic Act 3/2018. This is done both from a descriptive point of view, and from more analytical and explanatory positions. Previously, a situational approach is made that highlights the role currently played by the fundamental right to data protection within the framework of

a hyperglobalized Information Society. The approach, although it is preferably legal, is completed with sociological and political aspects.
Key words: Data protection, Regulation (EU) 2016/679, Organic Act 3/2018, fundamental rights, principles, lawfulness of processing, rights, controller, data protection officer, infringements and penalties.

1 INTRODUCCIÓN

La protección de datos se ha convertido en un elemento esencial para el adecuado funcionamiento social y político. Emerge como una respuesta jurídica frente al imparable avance del mundo digital y de todos los problemas que este puede originar en la vida de las personas. La Sociedad de la Información transita ahora por un segundo momento, amplificada por la hiperglobalización y redefinida por las tecnologías disruptivas que se están construyendo en la actualidad. Nunca como hasta este momento los derechos conectados con la privacidad han estado tan expuestos.

Como hemos sostenido, la finalidad del derecho en sentido objetivo, consistente en regular la vida en sociedad, exige realizar actualizaciones y reformas cuando la evolución social así lo determine. Solo de este modo las normas jurídicas se mantendrán eficaces. La materia de protección de datos es un ejemplo paradigmático de esta idea[1]. En efecto, los avances tecnológicos de hace cincuenta años dieron lugar a que los sistemas jurídicos reaccionaran y asentaran la inicial regulación específica de protección de datos. Un poco después se fue conformando la Sociedad de la Información, que gracias a la digitalización ha sido capaz de procesar de forma masiva y eficaz datos de todo tipo. Pero ya entrado el siglo XXI se percibieron cambios en dicha sociedad, en especial en su segunda década cuando la extensión de las redes sociales y el desarrollo de las citadas tecnologías disruptivas abocan a ese segundo momento de la Sociedad de la Información. La genérica automatización se encuentra a la vuelta de la esquina, y la inteligencia artificial queda a la espera de abrir otro período[2].

La Unión Europea percibió esta situación y en un proceso complejo alumbró una nueva normativa de protección de datos por medio del Reglamento 2016/679, 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 (en adelante RGPD, pues ya es común referirse a esta norma como Reglamento general de protección de datos)[3]. El 25 de mayo de 2018 comenzó a aplicarse este reglamento en todo el territorio de la Unión. En el propio RGPD se habla de que "la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales" (considerando 6). Y en el mismo lugar se reconoce que la tecnología permite usar datos "en una escala sin precedentes", "a escala mundial". Ello obliga a reforzar el control y la seguridad jurídica (considerando 7).

Y en España, en desarrollo de este RGPD, se dictó la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de derechos digitales (en adelante LOPDGDD). Se conforma así una especie de tándem normativo que habrá que tener en cuenta a la vez en el ámbito de la protección de datos en nuestro país.

El propósito de este trabajo es hacer un recorrido explicativo de los diez aspectos de esta nueva regulación que consideramos más relevantes (serán los puntos del 2 al 11, ambos incluidos). Por lo tanto, no se trata solo de una aproximación descriptiva, aunque, claro está, aportamos datos desde esa óptica, sino de hacer un abordaje más analítico. La atención preferente la prestamos al RGPD, como norma de referencia base, aunque en todo momento también atendemos a la LOPDGDD. Asimismo, puntualmente consideramos otra normativa.

2 DERECHO FUNDAMENTAL

La protección de datos se ha configurado como un derecho fundamental. Ello es el primer elemento de nuestro decálogo en este trabajo por poseer especial significación jurídico-política y social. Se integra así en el corpus de derechos que constituyen la base del orden político y de la paz social (art. 10.1 de la Constitución española). Los derechos fundamentales son la clave de bóveda sobre la que se asienta un sistema público y se convierten en elementos nucleares de la democracia, que no será verdaderamente tal si no se prevén y garantizan con corrección estos derechos. Conforman de este modo la raíz epistemológica de la sociedad y de los poderes públicos. También la protección de datos, que se conecta por esta vía con la propia dignidad de la persona.

El derecho a la protección de datos otorga a todas las personas una potestad de control de sus datos personales, entendidos estos como toda información que identifica o hace identificable a una persona. De este modo, empodera a la ciudadanía en el actual entorno cambiante y convulso, donde las capacidades del mundo digital son capaces de tratar datos como nunca se hubiera imaginado en el pasado. El Tribunal Constitucional español, en su famosa Sentencia 292/2000, hablaba del "derecho a controlar el uso de los datos", que atribuye a su titular un "haz de facultades" consistentes "en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos" (fundamento jurídico 5). De esta forma, a pesar de la afinidad con el derecho a la intimidad, el derecho a la protección de datos es diferente, pues tienen distinta función, objeto y contenido.

Es importante resaltar esta idea de la protección de datos como derecho fundamental, pues no nos encontramos ante un mero principio político o ético, o ante una recomendación de buen gobierno. Ni mucho menos. Estamos ante un verdadero derecho fundamental que presenta por ello un conjunto específico de garantías, las propias de un derecho fundamental[4].

Al lado de las garantías jurídicas, también funcionan otros tipos de requerimientos para proteger los derechos fundamentales. Por una parte, la ciudadanía debe cumplir la legalidad, lo que es especialmente intenso en el caso de los derechos fundamentales. Y, por otra parte, los responsables públicos asumen un deber adicional de respeto y protección de estos derechos (el art. 26 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, al regular los principios de buen gobierno, establece que los altos cargos a los que se aplican "promoverán el respeto a los derechos fundamentales y a las libertades públicas").

En la Unión Europea el derecho a la protección de datos está previsto en el artículo 8 de la Carta de Derechos Fundamentales y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. En España, por su parte, la protección de datos se derivó del artículo 18.4 de la Constitución gracias a la interpretación doctrinal[5] y a la jurisprudencia constitucional, sobre todo a través de la citada Sentencia del Tribunal Constitucional 292/2000[6].

La Unión Europea confía en la protección de datos para que las personas puedan hacer frente a las nuevas situaciones. No en vano, "el tratamiento de datos personales debe estar concebido para servir a la humanidad" (considerando 4 RGPD). Pero la Unión también es consciente de los retos cuando se afirma que "la magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa", además de que "la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes" (considerando 6 RGPD). El derecho fundamental a la protección de datos se ha convertido así en un elemento esencial de la convivencia democrática.

La LOPDGDD también evidencia las nuevas circunstancias cuando se lee, en el punto III de su preámbulo, que "los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización" han hecho que los datos personales "sean un recurso fundamental para la Sociedad de la Información".

En fin, como decíamos antes, esta segunda fase de la Sociedad de la Información, hiperglobalizada y tañida por las tecnologías disruptivas, avanza hacia un futuro diferente que necesita más que nunca del derecho a la protección de datos. Incluso habrá que sofisticar las categorías y regulaciones jurídicas para mantener su operatividad y para salvaguardar la vida privada en el escenario que se acerca.

Un último apunte antes de proseguir. Hay que tener en cuenta que no hay derechos fundamentales absolutos, tampoco el de protección de datos. Se pueden limitar cuando hay razones que lo justifican y que están previstas en el ordenamiento. Esta limitación, dicho ahora con sencillez, debe hacerse por un procedimiento basado en el principio de proporcionalidad. De lo que se trata en muchas ocasiones es de equilibrar los conflictos entre derechos para solucionar casuísticamente los problemas que vayan surgiendo y regular correctamente a la sociedad. Así, por ejemplo, el encuentro entre protección de datos y el derecho de acceso a la información pública se disciplina en el artículo 15 de la citada Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.

3 UNIFORMIDAD EUROPEA Y RECEPCIÓN EN ESPAÑA

El segundo elemento de nuestro decálogo es la apuesta de la Unión Europea por una norma como es el reglamento (el aludido RGPD[7]), el cual pretende imponer una uniformidad en la materia de protección de datos en todo el territorio de esa organización. Ello no se había conseguido con la norma de referencia anterior, la citada y ya derogada Directiva 95/46/CE, posiblemente por su propia naturaleza.

Debemos recordar que la norma europea conocida como reglamento presenta un alcance general, resulta obligatorio en todos sus elementos y se aplica directamente en cada Estado miembro. Tales características no las tiene la directiva[8]. O sea, que el reglamento posibilita una finalidad homogeneizadora que no permite la directiva. En este orden de cosas, el propio RGPD reconoce las diferencias en el nivel de protección de los datos al amparo de la Directiva 95/46 (considerando 9). Además, sostiene que para garantizar "un nivel coherente de protección" es necesario un reglamento que proporcione seguridad jurídica y transparencia (considerando 13).

En principio no es necesario que los Estados adopten un acto nacional de transposición de un reglamento europeo. Sin embargo, ello puede ser conveniente para ganar en certeza y seguridad

jurídica. Es el caso del RGPD, que en el supuesto español reclama una legislación nueva que depure el ordenamiento interno, dado que este posee previsiones que no se acomodan a aquel.

Apunta certeramente Jiménez Asensio que la derogación de la Directiva 96/45/CE y su sustitución por el RGPD "no es una operación normativa menor", sino motivada por el cambio de un contexto (tecnológico) en el que nuestra vida se está *datificando* (es decir, revelamos sin querer enormes cantidades de información)[9].

Dada la importancia de la materia regulada, la elaboración del RGPD fue compleja e intensa[10]. Ello se traduce en una norma extensa, alambicada y confusa en ciertos lugares. Como sostuvimos en otro trabajo, su carácter abigarrado "resulta sin ningún género de dudas una dificultad hermenéutica"[11]. También llama la atención el elevado número de remisiones al legislador nacional: más de cincuenta remisiones al derecho de los Estados, con lo que el desarrollo que comentábamos antes cobra otra justificación adicional. De igual modo, los muchos considerandos iniciales, que funcionan como una suerte de preámbulo (173), realizan una especie de interpretación auténtica e incluso proporcionan información adicional y distinta de la que consta en los artículos posteriores. Ello denota una incorrecta técnica legislativa.

El RGPD es para la Unión Europea un instrumento transcendental para dicha organización, en la actualidad y en el futuro. De este modo, se afirma que "el presente reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas" (considerando 2 RGPD). Parece depositarse en una correcta normativa de protección de datos la evolución de esta organización, tanto en términos jurídicos como sociales y económicos.

En todo caso, existen distintas materias fuera del RGPD, como veremos en el subapartado 11.1 de este trabajo, como los de la investigación policial y judicial en virtud de la Directiva 2016/680. Esta dualidad de previsiones se explica por la necesidad que en Europa se tuvo de aumentar la cooperación judicial y policial, lo que llevó a una norma específica como la citada directiva.

La recepción en España del RGPD se hace a través de la citada LOPDGDD. Se consideró, con buen criterio, que era preciso aprobar una nueva ley orgánica que sustituyese a la anterior de 1999. Como se lee en el punto III del preámbulo de la LOPDGDD, el principio de seguridad jurídica, por un lado, obliga a integrar el ordenamiento europeo de una manera clara y pública, y, por otro, implica la obligación de "eliminar situaciones de incertidumbre derivadas de la existencia de normas en el derecho nacional incompatibles con el europeo". Esto se traduce en la necesidad de eliminar la normativa interna incompatible con la norma europea. Estas razones fundan la necesidad de la LOPDGDD. Sin embargo, esta ha ido más allá del tema de protección de datos al abordar la cuestión de los derechos digitales. Estamos convencidos de que ello ha sido una mala técnica legislativa, pues debieron aprobarse dos leyes distintas, ya que ambos contenidos así lo reclamaban. Otra cosa será la transposición de la Directiva 2016/680, cuando esta se produzca.

Sea como fuere, el RGPD y la LOPDGDD se muestran hoy en día como un conjunto normativo sumamente interconectado, con referencias continuas entre ambos textos. Es de esperar que este conjunto sea decisivo en el devenir social y jurídico, además de ser tenido muy en cuenta por los responsables públicos y privados. El éxito de su aplicación, si se logra, será un avance en la convivencia democrática que a todos nos toca construir.

4 NUEVO PARADIGMA

El tercer punto de este decálogo es, ni más ni menos, el cambio de paradigma en el tema de protección de datos.

El anterior modelo era un sistema reactivo que descansaba en el control del cumplimiento y en la inscripción de ficheros en las agencias *ad hoc*. El nuevo modelo, en cambio, es de supervisión continua y cotidiana, proactivo, que obliga a los responsables y encargados de tratamiento a adoptar las medidas técnicas y organizativas necesarias para garantizar la protección de datos. Para ello deben analizarse los riesgos que pueden presentarse, antes de que se presenten, y estar ya preparados para la respuesta si se produce una brecha de seguridad. El destacado rol que deben desempeñar las autoridades de control se sitúa en la misma línea. No se trata de meros cumplimientos formales de las obligaciones, sino de asumir esta cultura de la responsabilidad activa, con lealtad y transparencia.

El entendimiento dinámico de este sistema proactivo se traduce en que las medidas adecuadas deben ser objeto de revisión y actualización cuando sea necesario (art. 24 RGPD), lo que atestigua que las medidas tomadas en cierto momento pueden anquilosarse y ser inútiles si no se someten a *aggiornamento*.

Esta mutación de modelo hace que la palabra "tratamiento" sea la correcta para reflejar la atención permanente que hay que articular, pues hace referencia al presente. Alude al empleo que los usuarios hacen de los datos en dicho tiempo presente. El reto va a estar en que las organizaciones sean capaces de imbuirse de la nueva mentalidad lo más pronto posible porque mantenerse en esquemas del pasado va a lastrar la protección de datos de forma inaceptable.

5 PRINCIPIOS

En el régimen de protección de datos existe un conjunto de principios que enmarcan todo tratamiento. Así los denomina el RGPD, aunque desde un punto de vista técnico-jurídico no todos sean realmente principios. Tales previsiones, que son el núcleo central del régimen jurídico de protección de datos, deben ser tenidas en cuenta en todo caso.

De esta forma, en el artículo 5 RGPD encontramos los denominados principios de lealtad y transparencia en el tratamiento de datos; limitación de la finalidad (o sea, solo se recogen datos para fines determinados, explícitos y legítimos); minimización de datos (solo se tratan los datos adecuados y pertinentes en relación con los fines); exactitud de los datos (los datos deben ser exactos, y, si no, hay que actualizarlos); limitación del plazo de conservación (no se deben guardar más del tiempo necesario para los fines de tratamiento); integridad y confidencialidad (mantener la seguridad de los datos); y responsabilidad proactiva (que ejemplifica el cambio de modelo visto en el apartado anterior).

La LOPDGDD aborda la cuestión en su título II, titulado "Principios de protección de datos", donde con gran imprecisión jurídica se abordan cosas diversas, como el deber de confidencialidad (que es obviamente un deber, no un principio), consentimiento de menores o datos especiales. Se puede destacar el artículo 4.2 LOPDGDD, que establece que en ciertos supuestos no será imputable al responsable de tratamiento la inexactitud de los datos personales siempre que haya adoptado todas las medidas razonables para que se supriman o rectifiquen. En concreto, cuando los hubiese obtenido directamente del interesado, o de un mediador o intermediario, o de otro responsable al ejercerse el derecho de portabilidad, o de un registro público.

| A&C | ISSN: 1887-0287 | Vol. 13_n. 2_2018 (xulio – decembro 2018) |

La ley española también precisa que el deber de confidencialidad es complementario de los deberes de secreto profesional y que siempre se mantienen "aun cuando hubiese finalizado la relación del obligado con el responsable" (art. 5.3 LOPDGDD).

6 BASES DE LEGITIMACIÓN

Un elemento relevante de la actual regulación europea de protección de datos es la existencia de seis supuestos generales en los que será posible tratar datos personales. Por ello, se puede hablar de que tales supuestos son las bases que justifican el tratamiento, o sea, que lo legitiman. El RGPD se refiere a "licitud de tratamiento".

Estos casos son un elenco cerrado, de manera que, fuera de los supuestos que expresamente permiten el tratamiento de los datos, este no estará autorizado, o sea, será ilegal (con la salvedad del régimen específico de las categorías especiales de datos, al que nos referiremos *infra*, en el apartado 11.2). En virtud del artículo 6.1 del RGPD, las condiciones que hacen lícito el tratamiento son las siguientes:

a) Consentimiento: "el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos".

b) Ejecución de un contrato: "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales".

c) Obligación legal: "el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"[12].

d) Urgencia vital: "el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física".

e) Interés público: "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

f) Intereses legítimos: "el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

La regla general del punto f) (interés legítimo) no se aplica al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Para ellas está destinada la base e), la de interés público. Ambos conceptos, el interés legítimo y el interés público, requieren concreción para precisar su verdadero significado, lo que se irá obteniendo a medida que se vayan aplicando. La LOPDGDD exige que el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos del responsable tiene que derivar "de una competencia atribuida por una norma con rango de ley" (art. 8.2 LOPDGDD).

El consentimiento es objeto de previsiones adicionales, lo que revela que se han intentado superar situaciones anteriores disfuncionales. Ahora se exige que el consentimiento para autorizar el tratamiento de datos debe ser libre, específico, informado e inequívoco, y un acto afirmativo claro (considerando 32 y art. 4.11 RGPD, art. 6.1 LOPDGDD). Se trata de huir de situaciones confusas del pasado, en las que las personas eran literalmente engañadas por las organizaciones que recababan sus datos. Se ha acabado la letra pequeña ilegible o las redacciones incomprensibles. Se trata de apostar por la lealtad de los que recaban los datos respecto a los interesados. Como afirma el Grupo del Artículo 29, el consentimiento solo puede ser una base jurídica adecuada "si se ofrece al interesado control y una capacidad real de elección con respecto a si desea aceptar

o rechazar las condiciones ofrecidas o rechazarlas sin sufrir perjuicio alguno"[13]. Si existe un importante desajuste entre los intervinientes en una recogida de datos, el consentimiento puede estar viciado por no ser realmente libre.

Si para el cumplimiento de un mismo fin o mismos fines es necesario llevar a cabo diversas actividades, el consentimiento debe darse para todas esas actividades de tratamiento (considerando 32 RGPD). Y, por supuesto, cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos (*ibidem*, e igualmente art. 6.2 LOPDGDD). O sea, el consentimiento es individualizado al requerirse para todas las finalidades que se persigan con el tratamiento.

Asimismo, "cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales" (art. 7.1 y considerando 42 RGPD). Esto obliga a los responsables a protocolizar el archivo de los consentimientos, aparentemente *sine die*, para lograr cumplir en el futuro con esa exigencia de prueba de consentimiento.

En todo caso, el carácter verdaderamente informado del consentimiento encuentra una destacada dificultad en la compleja comprensión de algunos procesos tecnológicos de tratamiento. A esto se refiere López Calvo al aludir a la adhesión a redes sociales, con cláusulas de privacidad extensas y farragosas[14]. La ayuda de las autoridades de control en esta tesitura se muestra como necesaria, para arrojar luz en esta oscuridad y aconsejar a los interesados.

Con el nuevo RGPD hay que entender que ya se excluye el consentimiento tácito[15], que antes era aceptado. En efecto, este reglamento europeo trata de huir de situaciones oscuras y defiende en sus considerandos el consentimiento como acto afirmativo "claro" (el mencionado considerando 32 RGPD). Se acepta cualquier declaración o conducta "que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales". Por lo tanto, "el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento".

El consentimiento de los menores de edad presenta unas previsiones específicas. Es de sobra conocido cómo el uso de la tecnología digital por los menores puede presentar riesgos para su socialización y formación. Ciertamente, la interacción entre menores y tecnología digital es problemática, lo que se refleja en los múltiples riesgos que se generan para su correcta socialización y formación[16]. Los menores, por sus características, requieren una protección adicional en el empleo de sus datos. Como señala el considerando 38 del RGPD, los niños "pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales". El peligro se advierte sobre todo en la utilización de datos de menores "con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y de la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño".

En este sentido, el artículo 8 del RGPD se rotula "condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información". Cuando estamos en el supuesto general del consentimiento para el tratamiento de datos (el del citado art. 6.1.a RGPD), en el caso de "oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años". Es decir, si el menor tiene 16 años o más puede consentir él por sí mismo. Puede y debe consentir, pues un tercero, como los padres, no puede sustituir ese consentimiento. En cambio, "si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó". No obstante, estas previsiones están en parte subordinadas al margen de apreciación nacional, ya que los Estados miembros "podrán establecer por ley una edad inferior

a tales fines, siempre que esta no sea inferior a 13 años". Amparándose en este margen de apreciación nacional que autoriza el reglamento, la LOPDGDD establece la barrera en 14 años (art. 7.1 LOPDGDD), aunque quedan a salvo los supuestos en los que una ley exija la asistencia de los titulares de la patria potestad para la celebración de un negocio jurídico. De este modo, "los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos" que veremos en el apartado siguiente (art. 12.6 LOPDGDD).

La importancia del tema del consentimiento de los menores reclama una diligencia adicional para los responsables de tratamiento. Además, se podrá aplicar el derecho de supresión de datos personales si el interesado, siendo ya adulto, dio su consentimiento siendo niño y no era plenamente consciente de los riesgos que implica el tratamiento, en especial en internet (considerando 65 RGPD).

7 DERECHOS

El derecho fundamental a la protección de datos contiene dentro de sí un grupo de derechos o subderechos que, como tales, atribuyen otras tantas facultades a los interesados. Puede parecer curiosa esta situación (un derecho que contiene derechos), pero también se produce en otros ámbitos (como el derecho a la tutela judicial, que presenta varios derechos en su interior).

Estos derechos concretan el control que los interesados deben tener sobre sus datos, con un haz de facultades que, desde el principio de autonomía de la voluntad, hacen posible adoptar diversas decisiones para no perder dicho control. Como decimos, los derechos se ejercen si así lo decide su titular, y como indica la LOPDGDD "directamente o por medio de representante legal o voluntario" (art. 12.1 LOPDGDD). Para facilitar estas acciones "el responsable de tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden" (art. 12.2 LOPDGDD).

En la configuración tradicional de la protección de datos estos derechos eran cuatro, que respondían al acrónimo ARCO. Se trataba de los derechos de acceso, rectificación, cancelación y oposición. Con el RGPD los derechos se amplían. El nuevo listado es el siguiente: derechos de información, acceso, rectificación, supresión, limitación de tratamiento, portabilidad, oposición, y no decisión única, además de otros derechos como los de presentar una reclamación ante la autoridad de control, o la tutela judicial contra una decisión de una autoridad de control, o también la tutela judicial frente a un responsable o encargado de tratamiento.

La LOPDGDD alude a los "derechos de las personas" en su título III, donde se concretan distintas cuestiones de su ejercicio. También el artículo 32 LOPDGDD incide en el tema de derechos, al especificar que cuando sea pertinente la rectificación o supresión de datos se procederá a su bloqueo. De relevancia práctica es la específica previsión de la información por capas: la información básica es a la que primero accederá la persona interesada, donde se indicará "una dirección electrónica y otro medio que permita acceder de forma sencilla e inmediata a la restante información" (art. 11.1 LOPDGDD).

Todo este conjunto de derechos fortalece la posición de la ciudadanía en este tema, que podrá acudir potestativamente a ellos para articular, como hemos dicho, distintas facultades. Todas estas facultades se hallan garantizadas con el sistema diseñado al efecto y que ahora se ve fortalecido por la dureza de las sanciones, a lo que nos referimos más abajo.

8 ESTRUCTURA INSTITUCIONAL

La correcta articulación de la protección de datos exige cierto entramado institucional específico. Nos vamos a referir ahora a este, y no a las estructuras orgánicas que sirven para la garantía de los derechos en general (y que ya citamos en la nota 4 de este artículo).

De esta forma, el RGPD apuesta por determinada estructura, con distintos sujetos, a los que dota de relevantes funciones para la buena marcha de la protección y gestión del tratamiento de datos personales. Se trata de una situación en gran parte novedosa con relación al régimen anterior, que obliga a las distintas entidades y organizaciones a replantearse su estructura para responder a las actuales exigencias.

8.1 Responsable y encargado de tratamiento

En primer lugar, tenemos al responsable de tratamiento de datos, que es quien determina "los fines y medios del tratamiento" (art. 4.7 RGPD). Puede ser una persona física o jurídica, o un organismo o servicio. Esta figura es la que asume las principales obligaciones en la materia, entre las que destacamos la adopción de las medidas técnicas y organizativas para garantizar la legalidad del tratamiento (art. 24.1 RGPD y art. 28.1 LOPDGDD) y un nivel de seguridad adecuado al riesgo (art. 32.1 RGPD).

El encargado de tratamiento será quien trate datos personales "por cuenta del responsable" anterior (art. 4.8 REDP). También puede ser una persona física o jurídica, o un organismo o servicio. Para regular la relación entre ambos, se prevé un contrato con un contenido detallado en el artículo 28.3 RGPD.

El nuevo modelo de protección de datos de responsabilidad activa exige que el responsable y el encargado valoren el riesgo que podría generar un tratamiento y así poder adoptar las medidas pertinentes ante esa situación concreta. Sobre ello volveremos en el punto 9 de este trabajo.

8.2 Delegado de protección de datos

El delegado de protección de datos es el asesor y fiscalizador en la materia de ciertas organizaciones y entidades que tratan datos, en concreto las que se citan en el artículo 37.1 RGPD y en el 34.1 LOPDGDD (como todas las autoridades públicas, salvo los tribunales). El nombramiento de este delegado le corresponde al responsable o al encargado de tratamiento, lo que deberá comunicarse a la autoridad de control. Su posición es de independencia, y no podrá recibir instrucciones (art. 38.3 RGPD). Además, debe participar en todas las cuestiones de protección de datos de la organización (art. 38.1 RGPD) e igualmente inspeccionar los procedimientos y emitir recomendaciones (art. 36.1 LOPDGDD). El delegado es el "interlocutor del responsable o encargado del tratamiento" ante la autoridad de control (art. 36.1 LOPDGDD).

La LOPDGDD, en su artículo 37, refuerza la posición del delegado al atribuirle la competencia de recibir y resolver reclamaciones de posibles afectados, lo que le acerca, curiosamente, a la naturaleza de un *ombudsman*. De esta forma, el afectado puede dirigirse al delegado de protección de datos de la entidad contra la que reclame antes de acudir a la autoridad de control. El delegado tiene dos meses para comunicar al afectado su decisión. Asimismo, la autoridad de control puede remitir una reclamación al delegado para que responda voluntariamente en el plazo de un mes.

Se trata de una figura inspirada en la institución del *compliance* del ámbito mercantil, aunque ha adquirido un creciente protagonismo, quizá excesivo, pues los focos deben caer sobre responsable y encargado, los verdaderos obligados para que el sistema actual funcione. En España su posición, en el caso de órganos públicos, debe cohonestarse con las previsiones del

Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, aprobado por Real decreto 3/2010, de 8 de enero (donde se contempla un responsable de seguridad, además de un responsable de la información y un responsable de servicios –art. 10–).

8.3 Autoridades de control

Cada Estado debe establecer una o varias autoridades públicas independientes para supervisar la aplicación del RGPD (art. 51.1 REDP). Su finalidad es tanto proteger los derechos y libertades de las personas físicas en el tratamiento de datos como facilitar la libre circulación de estos en el territorio de la Unión Europea. Están dotadas de funciones (art. 57 RGPD) y poderes (art. 58 RGPD) relevantes, entre los que se hallan los poderes correctivos, que incluyen sanciones y órdenes. La norma europea destaca esa posición de independencia en el artículo 52, en el cual se habla de "total independencia", de miembros "ajenos a toda influencia externa" que "no solicitarán ni admitirán ninguna instrucción", y de que cada Estado garantizará que cada autoridad de control disponga "en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios".

En España la autoridad de control nacional es la Agencia Española de Protección de Datos, prevista en la LOPDGDD en los artículos 44 y siguientes. Como autoridad administrativa independiente, está sujeta a la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público. El deber de colaboración con esta agencia que pesa sobre las administraciones públicas y los particulares está recogido en el artículo 52 LOPDGDD, precepto que alude a datos, informes, antecedentes y justificantes necesarios para llevar a cabo la actividad e investigación de la agencia. Este deber parece imprescindible para llevar a buen término las competencias de la agencia.

Además, en el ámbito autonómico tenemos órganos de este tipo en Cataluña (Autoridad Catalana de Protección de Datos) y País Vasco (Agencia Vasca de Protección de Datos), y en parte en Andalucía, aún pendiente de implementar alguna de sus competencias (Consejo de Transparencia y Protección de Datos). La LOPDGDD ampara la existencia de estas entidades autonómicas (arts. 57 y ss.), que deberán cooperar con la agencia estatal e intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones.

8.4 Comité Europeo de Protección de Datos

El último eslabón en el entramado institucional es el Comité Europeo de Protección de Datos (arts. 68 y ss. RGPD), un organismo de la Unión Europea que supervisa la aplicación del RGPD y asesora a la Comisión europea en el tema, además de, entre otras cosas, emitir directrices, recomendaciones y buenas prácticas. Asimismo, elabora un informe anual que hace público y transmite al Parlamento Europeo, al Consejo y a la Comisión.

En el Comité se integran los directores de las autoridades de control de los Estados miembros y el Supervisor Europeo de Protección de Datos. Sustituye al conocido como Grupo de Trabajo del Artículo 29 (que funcionaba con base en la Directiva 95/46/CE, derogada por el RGPD).

9 GESTIÓN DE ÍNDOLE PREVENTIVA

El modelo actual de protección de datos, como vimos en el apartado 4, es proactivo. Ello obliga al responsable a realizar una serie de labores que podrían calificarse de preventivas. De lo que se trata es de anticiparse a los problemas que puedan surgir y a las brechas de seguridad. Mejor evitarlas que responder después de que se produzcan. El modelo anterior, de control

del cumplimiento, implicaba actuaciones una vez que el problema ya había tenido lugar, para repararlo. Por ello, el paradigma actual, si funciona correctamente, es mucho más plausible.

En este sentido, citamos tres actuaciones que creemos que reflejan bien la idea que queremos transmitir. La primera es la elaboración del registro de actividades de tratamiento con las especificaciones que se exigen (art. 30 RGPD y art. 31 LOPDGDD). De lo que se trata sobre todo es de especificar "las actividades de tratamiento llevadas a cabo", o sea, de que el registro sea un fiel reflejo de la realidad del tratamiento de datos en la organización respectiva. Las entidades públicas citadas en el artículo 77.1 LOPDGDD deben hacer público un inventario de sus actividades de tratamiento (art. 31.2 LOPDGDD), lo que ya se ha incorporado como una obligación de transparencia activa en el artículo 6 bis de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en virtud de la disposición final undécima de la LOPDGDD). Esta publicación es una buena noticia para avanzar en el principio de transparencia. Además, téngase en cuenta que no llevar registro de actividades de tratamiento es una infracción grave (art. 73.n LOPDGDD); y que, si el registro no incorpora toda la información exigida, estamos ante una infracción leve (art. 74.l LOPDGDD).

La segunda actuación que ejemplifica la gestión preventiva es la realización de un análisis de riesgos para determinar las medidas concretas que se deberán articular para evitarlos (considerando 83 RGPD: "evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado"). Como hemos dicho *supra*, en el subapartado 8.1, esta labor permitirá al responsable y encargado del tratamiento aplicar las medidas técnicas y organizativas apropiadas (los ya citados art. 32.1 RGPD y art. 28.1 LOPDGDD). En este sentido, hay que tener en cuenta los "mayores riesgos" que podrían producirse en una serie de supuestos que fija el artículo 28.2 LOPDGDD (como el surgimiento de situaciones de discriminación, usurpación de identidad, fraude, pérdidas financieras, daño para la reputación, vulneración del secreto profesional o reversión no autorizada de la seudonimización; afectación a grupos en situación de especial vulnerabilidad; tratamientos masivos; o transferencias de datos a terceros Estados que no cuentan con un nivel adecuado de protección). Otra vez hay que tener presente, en el ámbito del sector público, que el ya citado Esquema Nacional de Seguridad también contempla, por su parte, un análisis y gestión de los riesgos (art. 13 del Real decreto 3/2010).

Y la tercera obligación de tipo preventivo que recogemos son las denominadas evaluaciones de impacto en las operaciones de tratamiento de datos (art. 35 RGPD). Estas deberán realizarse cuando un tratamiento entrañe un alto riesgo para los derechos y libertades. En concreto, proceden cuando se va a efectuar una "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado", un tratamiento a gran escala de categorías especiales de datos, o una "observación sistemática a gran escala de una zona de acceso público". Para realizar esta evaluación, el responsable recabará asesoramiento del delegado de protección de datos. Si se efectúa el tratamiento de datos personales sin haberse realizado la evaluación de impacto en los supuestos en que esta es exigible, se cometerá una infracción grave (art. 73.t LOPDGDD).

Estas gestiones preventivas, por lo tanto, evidencian la concreción del nuevo paradigma en el tratamiento de datos y el cambio de la lógica organizacional.

10 INFRACCIONES Y SANCIONES

El derecho, en sentido objetivo, tiene como uno de sus elementos característicos la coactividad, esto es, la posibilidad de ser impuesto por la fuerza. Si las normas jurídicas no se cumplen voluntariamente, el sistema público tiene mecanismos de imposición. Esta idea es de suma relevancia en el campo de los derechos fundamentales, pues de poco sirve su reconocimiento teórico si después no se establecen medios y fórmulas para garantizar su aplicación. Las garantías de los derechos son una exigencia de la técnica jurídica y también de la propia calidad de la democracia. Es más, los instrumentos de garantía se tienen que actualizar cuando corresponda para que las nuevas situaciones no afecten negativamente a la aplicación de los derechos.

El derecho a la protección de datos tiene, como hemos mencionado *supra*, las garantías de los derechos fundamentales en general. Pero, además, el RGPD y la LOPDGDD aluden a unas infracciones y sanciones concretas ante las vulneraciones de la protección de datos. Esto supone un endurecimiento del sistema de sanciones dado lo elevadas que pueden resultar ahora las multas. Así, se habla en su nivel máximo de multas administrativas de 20 millones de euros o del 4% del volumen de negocio total anual de una empresa, "optándose por la de mayor cuantía" (art. 83.5 RGPD).

La LOPDGDD aborda el procedimiento a seguir ante una vulneración de protección de datos (arts. 63 y ss.) y el régimen sancionador, tanto en lo que atañe a sujetos responsables como a infracciones y sanciones (arts. 70 y ss.). Se describen las conductas típicas y se gradúan las infracciones entre muy graves, graves y leves, gradación que se hace para determinar los plazos de prescripción. De igual modo, se fija la interrupción de dicha prescripción (art. 75 LOPDGDD).

En este sentido, es de reseñar que los responsables de órganos públicos no serán sancionados económicamente, sino que se castigarán a través de apercibimientos, actuaciones disciplinarias o amonestaciones, aunque todo ello con publicidad y con aviso al Defensor del Pueblo o a los defensores autonómicos (art. 77 LOPDGDD). Por lo tanto, en estos supuestos se sustituyen las multas por la publicitación del infractor, lo que en determinados casos puede ser una técnica de prevención de infracciones muy eficaz. Pese a ello, hay quien considera que este régimen especial es un privilegio del sector público, con lo que no estamos de acuerdo.

11 UNA REGULACIÓN COMPLEJA

Uno de los rasgos que se podrían considerar característicos de la protección de datos es el de su heterogeneidad y complejidad. Es el último elemento de nuestro decálogo. Las causas de esta complejidad las centramos en tres: la habitual existencia de excepciones a las previsiones generales, la previsión de ámbitos excluidos y de regulaciones específicas, y lo que podemos calificar como sectores regulados de manera más flexible.

11.1 Materias excluidas y regulaciones específicas

En primer lugar, hay que tener presente el ámbito de aplicación material de la normativa. En este sentido, el RGPD, en su artículo 2.2, indica que no se aplica a actividades no comprendidas en el derecho de la Unión, a la política exterior y de seguridad común de la Unión, y a las actividades exclusivamente personales o domésticas.

Sin embargo, en una muestra de mala sistemática, en otros lugares el RGPD también aborda cuestiones referidas a su ámbito a aplicación. Así, el RGPD no se aplica a los datos personales de las personas fallecidas según interpretan sus considerandos (considerandos 27, 158 y 160); ni a las personas jurídicas (considerando 14, aunque esto también se puede interpretar por el propio

enunciado del RGPD); en el tratamiento de datos en las instituciones, órganos y organismos de la Unión Europea se aplica la normativa específica de ese ámbito, que debe adaptarse al nuevo régimen (art. 98 RGPD)[17]; tampoco se aplica el RGPD en tratamientos objeto de la citada Directiva (UE) 2016/680 (considerando 19 RGPD)[18]; con relación a las comunicaciones electrónicas se aplica prioritariamente la Directiva 2002/58/CE, y el RGPD de forma supletoria sin imponer obligaciones adicionales (art. 95 RGPD y considerando 173)[19]; y respecto al comercio electrónico también se aplica prioritariamente la Directiva 2000/31/CE[20] (considerando 21 RGPD).

Por su parte, la LOPDGDD no es de aplicación a los tres supuestos anteriores del citado artículo 2.2 RGPD y, además, a los tratamientos de personas fallecidas[21] (lo que ya interpretaban los considerandos vistos del RGPD) y a los tratamientos sometidos a la normativa de materias clasificadas (art. 2.2 LOPDGDD). La ley española, con relación a las actividades no comprendidas en el derecho de la Unión, alude a que esos tratamientos se regirán por su legislación específica, como es el caso del régimen electoral general o el Registro Civil (art. 2.3 LOPDGDD). Sorprende que se pongan ejemplos en la redacción de un artículo de una ley, pero ahí están.

Realmente en estos elencos citados en los párrafos anteriores hay dos tipos de supuestos. Uno, el de las materias a las que no se aplica la protección de datos, que podríamos calificar como ámbitos excluidos. Se trata, por ejemplo, de las actividades personales o domésticas y de los tratamientos de personas fallecidas. Y los otros supuestos son los que se rigen por sus disposiciones específicas, como el caso de las instituciones europeas o las actividades no comprendidas en el derecho de la UE. En este segundo tipo tenemos supuestos en los que se aplica la norma específica y no el RGPD (como en investigación policial) y otros en los que el RGPD entra como norma de aplicación supletoria (como en comercio electrónico o en comunicaciones electrónicas).

Un supuesto con características propias es el ámbito judicial. Aunque el reglamento europeo se aplica a las actividades de los tribunales, las autoridades de control no son competentes para supervisar las operaciones de tratamiento "efectuadas por los tribunales en el ejercicio de su función judicial" (considerando 20 y art. 55.3 RGPD). El control de tales tratamientos depende de los órganos a los que se atribuya esa competencia dentro del sistema judicial (en el caso español el Consejo General del Poder Judicial, como así lo establece el artículo 236 *nonies* de la Ley orgánica 6/1985, de 1 de julio, del poder judicial).

11.2 Excepciones

En este subapartado nos estamos refiriendo a situaciones en las que existe una regulación general que se acompaña de una previsión que se aparta de ella. Lógicamente, ahora no podemos hacer un repaso por todas estas excepciones a las disposiciones generales que están previstas en la normativa de protección de datos. Aludimos tan solo a tres ejemplos que creemos que ilustran perfectamente la cuestión.

El primer ejemplo ya lo hemos visto antes: el consentimiento de menores, que puede entenderse como una excepción a las previsiones generales de la categoría del consentimiento. Remitimos al apartado 6 de este trabajo.

En las transferencias de datos personales a terceros países u organizaciones internacionales, se regulan excepciones para situaciones específicas (art. 49 RGPD). De esta forma, en ausencia de una decisión de adecuación o de garantías adecuadas, se podrá realizar una transferencia de datos personales si es de aplicación alguna de las siete excepciones que enumera tal precepto (como consentimiento explícito, ejecución de un contrato o razones de interés públicos).

De igual forma, el tratamiento de los llamados datos especiales también puede considerarse una excepción a la regulación general de los datos (no especiales, por tanto). Los datos especiales, que son la evolución de lo que antes en castellano se llamaban datos especialmente protegidos, se refieren a cuatro tipos de datos (art. 9.1 RGPD): los de origen étnico o racial; las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical; el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, y datos relativos a la salud; y datos sobre la vida sexual o la orientación sexual de una persona física. Como indica la norma europea, los datos especiales son "particularmente sensibles en relación con los derechos y libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos" para estos derechos y libertades (considerando 51 RGPD).

Así las cosas, el artículo 9.1 del RGPD establece la prohibición genérica de tratar los datos especiales, si bien ello presenta diez excepciones (art. 9.2 REDP). De una forma sintética, estas excepciones son el consentimiento explícito del interesado[22]; el cumplimiento de obligaciones del responsable en el ámbito laboral; la protección de intereses vitales del interesado; tratamiento de una entidad política o religiosa respecto a sus miembros; datos que "el interesado ha hecho manifiestamente públicos"; tratamiento necesario para las actuaciones judiciales; razones de "un interés público esencial"; fines de medicina preventiva o laboral; salud pública o garantía de la calidad de la asistencia sanitaria; y fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

El consentimiento que se exige en este caso de los datos especiales, como acabamos de decir, es "explícito"[23], lo que supone un paso más con relación al consentimiento inequívoco que comentamos en las reglas generales en el apartado 6 de este trabajo. Por lo tanto, ante tratamiento de datos no especiales hay que interpretar que cabe un consentimiento implícito (pues el explícito solo se cita para los datos especiales), que en todo caso será inequívoco, específico y claro, como reclama el propio concepto de consentimiento que en todo caso maneja el RGPD (o sea, no tácito).

11.3 Ámbitos flexibilizados

Nombramos así este subepígrafe para aludir a un conjunto de sectores que presentan previsiones más flexibles. Podrían ser también excepciones a la regulación general, que acabamos de ver, pero para ganar fuerza explicativa los consideramos al margen.

El RGPD le dedica el capítulo IX a lo que rotula como "Disposiciones relativas a situaciones específicas de tratamiento". Esto se refiere a ciertos tratamientos concretos que por ello necesitan una previsión *ad hoc*. En ese lugar se contemplan tres supuestos en los que las previsiones son menos rígidas: la conciliación de la protección de datos con la libertad de expresión e información (art. 85 RGPD); el tratamiento para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (art. 89 RGPD); y la protección de datos en las iglesias y asociaciones religiosas (art. 91 RGPD)[24].

12 CONCLUSIONES

Tras el decálogo expuesto, creemos que queda reflejada la importancia que posee en la actualidad la protección de datos, como garantía frente al avance arrollador de la Sociedad de la Información, y la propia complejidad de ese sector del ordenamiento, con regulaciones detalladas, exclusiones y previsiones específicas en varios ámbitos, quizá excesivas y abigarradas.

La nueva normativa ha concretado más aspectos, cambiado el modelo y endurecido algunas previsiones (como en los requisitos del consentimiento y en las posibles sanciones). Se busca con todo ello superar problemas del pasado y proteger de forma efectiva a la ciudadanía frente a las grandes corporaciones y entidades. Las ideas de lealtad y transparencia retratan bien la nueva situación que se persigue, con obligaciones concretas para responsables y encargados de tratamiento en ese sentido, y con acciones proactivas que deberían evitar problemas futuros o, si estos se producen, asegurar una respuesta adecuada.

De todos modos, tenemos ciertas reservas sobre el éxito real de la normativa que regula la protección de datos. Un sinfín de escándalos que afectan a la privacidad de las personas ocupan las primeras planas de los medios cada cierto tiempo en los últimos años. Estos casos rebelan cómo se comercia con los datos, su importancia económica y política, los continuos engaños a los que se ve sometida la ciudadanía o la falta de escrúpulos de algunos dirigentes de grandes empresas. El ejemplo de *Cambridge Analytics* vale por todos. Y después están los casos que no salen en los medios, las actuaciones secretas de ciberguerra y de inteligencia, que también en distintos momentos pivotan en torno a datos personales.

La ciberseguridad se irá progresivamente complicando, con lo que el escenario para el derecho fundamental de la protección de datos se hará más agresivo. Las tecnologías disruptivas dificultarán el control de nuestros datos y posiblemente reclamarán una actualización de la normativa que repasamos en este trabajo para regular cómo robots, máquinas, algoritmos o la todavía imprevisible computación cuántica podrán, o no, tratar nuestros datos, un bien precioso de la dignidad que cualifica al ser humano. La fortaleza de nuestra sociedad y de nuestra democracia está en juego, por lo que la forma de aplicar y de evolucionar el régimen de protección de datos será determinante en la concreción de la nueva dinámica social.

13 BIBLIOGRAFÍA

Fernández Rodríguez, J.J. 2004. *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*. México D.F.: Universidad Nacional Autónoma de México. Disponible en https://biblio.juridicas.unam.mx/bjv/detalle-libro/1167-lo-publico-y-lo-privado-en-internet-intimidad-y-libertad-de-expresion-en-la-red

Fernández Rodríguez, J.J. 2018. «Aproximación general a la reforma normativa: el reglamento europeo. Principios generales», en C. Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*. Madrid: Wolters Kluwer.

Grupo de Trabajo del Artículo 29. 2017. *Directrices sobre el consentimiento en el sentido del Reglamento UE 2016/679*. Disponible en

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Jiménez Asensio, R. 2018. «Epílogo», en C. Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*. Madrid: Wolters Kluwer.

Lázaro González, I.E.; Mora Prato, N., y Sarzano Volart, C. (coords.) 2012. *Menores y nuevas tecnologías*. Madrid: Tecnos.

López Aguilar, J.F. 2015. «Data Protection Package y Parlamento Europeo», en A. Rallo Lombarte y R. García Mahamut (eds.), *Hacia un nuevo Derecho Europeo de protección de datos*. Valencia: Tirant lo Blanch.

López Álvarez, L.F. 2016. *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo*. Madrid: Lefebvre.

López Calvo, J. 2017. *Comentarios al reglamento europeo de protección de datos*. Madrid: Sepin.

Lucas Murillo, P. 1990. *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

PricewaterhouseCoopers LLP. 2018. *Will robots really steal our jobs? An international analysis of the potential long term impact of automation*, disponible en

https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impact_of_automation_on_jobs.pdf

NOTAS

1 Fernández Rodríguez, 2018: 33.

2 Entre otros, puede verse el informe de PricewaterhouseCoopers LLP, 2018. Nosotros ya abordamos y vislumbramos esta problemática hace años (Fernández Rodríguez, 2004) partiendo de la afectación de la libertad de expresión y del derecho a la intimidad.

3 En el apartado 11 de este trabajo aludimos a otras normas de la Unión Europea que se añaden a este RGPD en la regulación de nivel secundario europeo en la materia.

4 De manera breve podemos clasificar las garantías de los derechos en normativas (reserva de ley, respeto al contenido esencial, eficacia inmediata, rigidez constitucional), jurisdiccionales (amparo "ordinario", amparo constitucional) e institucionales (Ministerio Fiscal, Defensor del Pueblo, defensorías autonómicas).

5 Lucas Murillo, 1990.

6 La primera ley orgánica española específica fue la 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, que fue sustituida por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. La LOPDGDD deroga esta ley de 1999 (aunque permanecen de momento en vigor los artículos 22, 23 y 24 de la Ley orgánica 15/1999, en virtud de la disposición adicional decimocuarta y disposición transitoria cuarta de la LOPDGDD).

7 El precedente directo de este RGPD fue la Comunicación de la Comisión, de 4 de noviembre de 2010, titulada "Un enfoque global de la protección de los datos personales en la Unión Europea".

8 La directiva obliga a los Estados destinatarios en cuanto al resultado. Es decir, sobre estos Estados pesa tal obligación de resultado, pero ellos eligen la forma y los medios para alcanzar dicho resultado. Por eso se dice que el legislador nacional debe adoptar un acto de transposición en el derecho interno que adapte la legislación nacional a los objetivos de la directiva. En este proceso, los Estados tienen cierta discrecionalidad, que les sirve para tener en cuenta las particularidades nacionales.

9 Jiménez Asensio, 2018: 628.

10 López Aguilar, 2015.

11 Fernández Rodríguez, 2018: 54.

12 El artículo 8.1 LOPDGDD prevé que esta obligación legal debe estar prevista en una norma de derecho de la Unión Europea o en "una norma con rango de ley".

13 Grupo de Trabajo del Artículo 29, 2017: 3.

14 López Calvo, 2017: 131 y ss.

15 Sin embargo, se ha defendido que este consentimiento sí cabe, pues se considera compatible con una conducta clara y afirmativa (*v. gr.*, López Calvo, 2017: 124 –aunque en la p. 129 parece sostener otra cosa–). Nosotros no opinamos así, como tampoco los legisladores nacionales que están desarrollando el RGPD: de esta forma, en España, en el punto V del preámbulo de la LOPDGDD se dice literalmente que este consentimiento de la norma europea excluye "lo que se conocía como consentimiento tácito".

16 Una visión de estos problemas, pero también de las oportunidades, puede verse en Lázaro González *et al.*, 2012.

17 La principal referencia es el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE. Este reglamento ya está adaptado al nuevo marco.

18 Recordemos que esta Directiva (UE) 2016/680 se refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. A través de ella se deroga la Decisión marco 2008/977/JAI del Consejo. La transposición de esta directiva en España está pendiente. Tal directiva no solo establece normas para proteger a las personas físicas en su objeto material, sino que también garantiza la libre circulación de datos personales en la Unión en el ámbito de la cooperación judicial en materia penal y en el de la cooperación policial.

19 Una previsión similar se encuentra en la disposición adicional undécima de la LOPDGDD.

20 Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

21 El artículo 3 LOPDGDD contiene previsiones específicas sobre los datos de personas fallecidas, relativas al acceso de los herederos o representantes.

22 El artículo 9.1 LOPDGDD preceptúa con relación a este caso que "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico".

23 Como afirma el Grupo del Trabajo del Artículo 29, "el consentimiento explícito se requiere en determinadas situaciones en las que existe un grave riesgo en relación con la protección de los datos y en las que se considera adecuado que exista un elevado nivel de control sobre los datos personales" (Grupo de Trabajo del Artículo 29, 2017: 20).

24 En cambio, otras previsiones en ese lugar del RGPD son más exigentes con relación a la normativa genérica (por lo tanto, no son ámbitos de tratamiento flexibilizados): acceso a documentos oficiales, tratamiento del número nacional de identificación, tratamiento en el ámbito laboral, y obligaciones de secreto para reforzar los poderes de las autoridades de control. Por su parte, la LOPDGDD también alude a algo similar en su título IV "Disposiciones aplicables a tratamientos concretos", aunque los casos que cita son como los de esta nota, más exigentes.