La transparencia en el nuevo Reglamento General de Protección de Datos

Transparency in the new General Data Protection Regulation

Elena García-Cuevas Roque

Académica Correspondiente de la Sección de Derecho de la Real Academia de Doctores de España.
garciacuevaselena@gmail.com

An. Real. Acad. Doct. Vol 3, (2018) pp. 64-79.

RESUMEN	ABSTRACT
La globalización y la vertiginosa evolución tecnológica abren nuevos retos para la protección de los datos personales. En un mundo digital, la transparencia pública es necesaria en aras de una "buena administración", pero ello no debe implicar automáticamente la disminución de las garantías de los ciudadanos en la esfera privada. La Sociedad de la Información exige un continuo intercambio de información entre los Estados, lo que puede dañar la privacidad de las personas. La Unión Europea ha asumido esta responsabilidad a través del Reglamento General de Protección de Datos, el cual contempla, por un lado, y como nuevo principio, la transparencia, con el fin de facilitar la comprensión de las políticas de privacidad e informar adecuadamente sobre el tratamiento de los datos; por otro, incluye entre los derechos del interesado, como si se tratara de un valor máximo, la transparencia de la información que favorecerá la toma de decisiones del ciudadano, sin olvidar, en este último caso, los riesgos que ello pueda suponer para los derechos fundamentales de la persona. Seguimos inmersos en la lucha por inculcar una "cultura de protección de datos en Europa" y conseguir el ansiado equilibrio entre protección de datos y derecho de acceso a la información pública.	Globalization and the rapid technological evolution open new challenges for the protection of personal data. In a digital world, public transparency is necessary for the sake of "good administration", but this should not automatically imply a reduction in the guarantees of citizens in the private sphere. The Information Society requires a continuous exchange of information between States, which can damage the privacy of people. The European Union has assumed this responsibility through the General Data Protection Regulation, which contemplates, on the one hand, and as a new principle, transparency, in order to facilitate the understanding of privacy policies and adequately inform about the treatment of the data; on the other hand, it includes among the rights of the interested party, as if it were a maximum value, the transparency of the information that will favor the citizen's decision making, without forgetting, in the latter case, the risks that this may entail for the rights fundamentals of the person. We are still immersed in the struggle to inculcate a "culture of data protection in Europe" and achieve the long-awaited balance between data protection and the right of access to public information.

Palabras clave: Transparencia, Reglamento general, protección de datos, acceso información, Europa	**Keywords:** Transparency, general regulation, data protection, access information, Europe

SUMARIO

1. INTRODUCCIÓN

Los avances tecnológicos reportan grades ventajas, pero también potenciales riesgos y peligros, máxime cuando asistimos a la difusión de un volumen cada vez mayor de informaciones personales.

La transparencia se sustenta en dos pilares básicos: el acceso a la información y la publicidad activa; el límite en ambos casos es la protección de datos personales. El problema de la publicidad activa está planteando casos muy interesantes de Derecho Constitucional; no hay que olvidar, además, que el acceso a la información tiene su anclaje en el art. 105 CE[1], que obliga al legislador a regular dicho acceso, estableciendo unas salvedades: cuando afecte a la seguridad del Estado, la averiguación de los delitos y la intimidad de las personas.

Pero la transparencia pública encuentra su principal y general límite en la protección de datos. Mantener este difícil equilibrio es el reto en el que estamos inmersos.

Desde este punto de vista, contamos ya con interesantes y recientes sentencias del TEDH[2] y del TJUE[3] en materia de acceso a la información y protección de datos,

[1] Este precepto debe ponerse en conexión con el art. 20 CE. Pero no es el momento de tratar este aspecto.

[2] Recordemos, por su interés, la sentencia de la Gran Sala del TEDH de 8 de noviembre de 2016 (caso *Magyar*); versa sobre una ONG, que lleva este nombre -*Magyar Helsinki Bizottság*-, que supervisa la aplicación de las normas internacionales de derechos humanos de Hungría. El TEDH aborda frontalmente la cuestión del derecho de acceso a la información; para ello, elabora un test para saber si el derecho de acceso a la información tiene o no la protección de derecho fundamental en cada caso. De una forma categórica afirma que cuando quien tiene la información es un periódico o una ONG, se aplica el art. 10 del Convenio Europeo, relativo a la libertad de expresión e información. Sobre esta sentencia, puede consultarse el magnífico trabajo de Cotino Hueso, L., 2017. "El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental". En *Teoría y Realidad Constitucional,* núm. 40. UNED, pp. 287-290.

algunas de las cuales serán referenciadas en notas a pie de página. La revolución tecnológica y la digitalización del tratamiento de los datos personales han intensificado la labor de estos Tribunales, fundamentalmente del TJUE, completando su ya amplia doctrina jurisprudencial en el ámbito de los derechos fundamentales con pronunciamientos de gran calado y significación en la protección de los derechos de la privacidad y "sociedad en red".

La Directiva 95/46 supuso un auténtico hito en materia de protección de datos personales y de los derechos fundamentales en la UE, como sistema más avanzado del mundo; pero el vertiginoso desarrollo de las tecnologías hizo necesario su reforma. Aunque se habla de Nuevas Tecnologías en sentido amplio, la Red de redes, Internet, ha sido el principal recurso por su propia naturaleza global. No debe olvidarse que cuando un servicio es público, la persona no es el cliente; es un producto.

Constantemente se dice que las Nuevas Tecnologías han transformado la vida social y, sin duda, la economía. Gran parte del comercio de servicios está habilitado por las tecnologías digitales y los flujos de datos asociados. Dentro de la UE es necesario, entonces, un Reglamento que aporte la necesaria confianza a través de un marco sólido y coherente para la protección de datos; sólo así se proporcionará "seguridad jurídica y transparencia a los operadores económicos" y se ofrecerá a las personas físicas de todos los Estados miembros "el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento".

Pues bien, el Reglamento General de Protección de Datos[4] (en lo sucesivo, RGPD) ha sido el resultado de esa adaptación, fruto del compromiso asumido por el

[3] Éste ha venido sentando en los últimos años una jurisprudencia sólida, coherente e incisiva en el marco de la consagración de los derechos a la vida privada y de privacidad, ejerciendo una clara influencia sobre los Tribunales Constitucionales nacionales y los poderes judiciales de los Estados Miembros. No olvidemos ese "diálogo dinámico entre Tribunales" que alimenta la cultura de un Derecho Común europeo. Cfr., López Aguilar, J. F., 2017. "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU". En *Teoría y Realidad Constitucional,* núm, 39. UNED, pp. 559 y 561. Este autor nos deleita con jugosos comentarios en torno a dos sentencias de la Gran Sala del TJUE: la sentencia de 8 de abril de 2014 (Caso *Digital Rights Ireland*) y la sentencia de 6 de octubre de 2015 (Caso *Schrems -Maximilian Schrems v. Data Protection Commissioner-*).

[4] Reglamento (UE) 2016/679. Las autoridades europeas han ido elaborando fichas informativas y directrices para facilitar su cumplimiento y aplicación, aclarando algunos aspectos de la nueva normativa europea de protección de datos. De entre ellas, destacan las Directrices sobre la Transparencia a efectos del Reglamento 2016/679 (WP260), adoptadas el 28 de noviembre de 2017, si bien, al cierre de este trabajo, está pendiente todavía de consulta pública. Puede verse en http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp260_enpdf.pdf [Fecha de consulta: 22.12.2017]

Parlamento Europeo[5] y el Consejo de la Unión Europea. Dicho Reglamento persigue garantizar una supervisión coherente del tratamiento de datos personales, así como un nivel elevado -o como mínimo, uniforme, equivalente y adecuado- de protección de los datos de las personas físicas en toda la Unión, basada en la cooperación efectiva. De este modo, se evitarán divergencias que puedan entorpecer la libre circulación de datos[6].

2. ASPECTOS MÁS RELEVANTES DEL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El RGPD, aplicable a partir del 25 de mayo de 2018[7], constituye una de las normas de Derecho europeo de mayor transcendencia e importantes consecuencias, al alcanzar, en principio, a "todos" los ciudadanos de la Unión Europea y dibujar, con gran eficacia y en un entorno muy homogéneo (el europeo), un nuevo modelo de privacidad. En este sentido, supone un auténtico reto para los que actúan como responsables y encargados del tratamiento (Piñar Mañas, 2016: 9).

Este Reglamento, al tener alcance general y ser obligatorios todos sus elementos, es directamente aplicable a cada Estado de la UE, sin que sea necesaria transposición alguna, aunque pueden precisar desarrollo. En mayo de 2018 se abroga, tras veinte años de vigencia, la Directiva 95/46/CE que, como sabemos, fue el punto de partida a nivel europeo en materia de protección de datos; sin embargo, la mayoría de los objetivos y principios generales reguladores del régimen jurídico de los tratamientos, recogidos en la misma, siguen siendo válidos, sin desconocer que el paso de los años ha dejado constancia de la existencia de divergencias en la ejecución y aplicación de aquella Directiva.

El Parlamento Europeo y el Consejo de la Unión Europea han sido conscientes de las dificultades de garantizar adecuadamente el derecho fundamental a la protección de datos personales en un mundo digital; y aquellas divergencias en la aplicación de la Directiva han llevado a la necesidad de reformar ésta, pues "el tratamiento de los datos personales debe ser concebida para servir a la humanidad" (Considerando 4 RGPD), así como estar al servicio de todas las personas físicas y su bienestar, superando las fronteras. En definitiva, y tal y como

[5] Conviene recordar aquí la extraordinaria labor que ha efectuado el Parlamento Europeo en los últimos años en relación con el *Data Protection Package o* Paquete de Protección de Datos de la UE; fue necesaria una revisión de las normas de protección de datos de la UE promulgadas en 2016 y las implicaciones para las transferencias de datos entre el Reino Unido y la UE post-Brexit.

[6] En este sentido, el Considerando 13 RGPD hace referencia al mencionado marco sólido de protección de datos.

[7] Se concede, así un período de dos años para que los tratamientos iniciados con anterioridad se ajusten a sus disposiciones.

hemos señalado en la introducción de este trabajo, el Reglamento europeo "facilitará la actividad empresarial y corporativa transfronteriza, la libre circulación de datos personales y la mayor garantía de los derechos y libertades fundamentales de los ciudadanos europeos" (Díaz Díaz, 2016).

Pero, cabe preguntarse, en qué lugar queda la LOPD (y su Reglamento de desarrollo); la Ley Orgánica 15/1999 no debe considerarse derogada, aunque sí desplazada por el nuevo Reglamento y, posiblemente, exigirá su modificación. El RGPD reconoce también "un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales (<<datos sensibles>>)" (Considerando 10 RGPD), sin olvidar que, cuando sea necesario por razones de coherencia, aquellos Estados "pueden incorporar a su Derecho nacional elementos del RGPD".

Las principales novedades, a título de muestra, pueden condensarse en los siguientes puntos:

- Consolida definitivamente el derecho a la protección de datos como un derecho fundamental.

- Regula algo tan necesario en un mundo digital como el derecho de supresión o "derecho al olvido" (*Right to be forgotten*); la Agencia Española de Protección de Datos fue pionera en este aspecto[8] y el Derecho europeo supuso un importante refuerzo al mismo.

- Contempla el principio de la "responsabilidad proactiva" o rendición de cuentas aplicada a la protección de datos personales (*accountability*)[9], superando el modelo anterior estrictamente sancionador.

[8] La AEPD venía ya aplicando en sus resoluciones el denominado "derecho al olvido", llegando la cuestión al TJUE (caso *Google contra Agencia Española de Protección de Datos*), concluyendo aquél, el 13 de mayo 2014, que existe un derecho al borrado de nuestra información en Internet. De este modo, se reconoce que el tratamiento de datos que realizan los motores de búsqueda está sometido a las normas de protección de datos de la UE. "La tecnología lleva a la humanidad a la memoria como principio general y al olvido sólo por defecto", Rallo Lombarte, A. (Ed.), 2014. *El derecho al olvido en Internet. Google versus España.* Centro de Estudios Políticos y Constitucionales, Madrid, p. 17, cuya lectura recomendamos.

[9] Ya nos advierte Carrera Mariscal, Andrea que este principio no "nace" con la entrada en vigor del RGPD. Las líneas directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) del 23 de septiembre de 1980, revisadas en 2013, tanto como la recomendación del Grupo de trabajo sobre protección de datos del Artículo 29 adoptado el 13 de julio de 2010 se refieren a este principio como una herramienta de regulación compartida en el servicio de protección de datos personales. "El RGPD: el nuevo Reglamento europeo sobre la protección de datos personales basado en el principio de *Accountability*", en *The privacy advisor*, 28 de julio de 2016. https://iapp.org/news/a/el-rgpd-el-nuevo-reglamento-europeo-sobre-la-proteccion-de-datos-personales-basado-en-el-principio-de-accountability/. [Fecha de consulta: 15.11.2017].

- Regula el nuevo derecho a la portabilidad de los datos de responsable a responsable -cuando sea técnicamente posible-, para lo cual, ha sido de gran utilidad las aportaciones del Grupo de Trabajo del Artículo 29.

- Incluye el principio de la privacidad desde el diseño y por defecto, que también debe tenerse en cuenta en el contexto de los contratos públicos. En este punto, el principio de transparencia juega, asimismo, un papel muy relevante[10].

- Destaca la no exigencia de la inscripción de ficheros, si bien el responsable debe llevar un registro de actividades y notificar todas aquellas violaciones de seguridad.

- Introduce la nueva figura del Delegado de protección de datos, designado por el Responsable y el encargado del tratamiento, pero independiente de éstos, y con obligación de secreto y confidencialidad. Esta figura adquiere un indudable protagonismo en lo que concierne al respeto a la privacidad, y ayudará al responsable y al encargado del tratamiento a "garantizar una rendición de cuentas eficaz".

3. PRINCIPIOS RELATIVOS AL TRATAMIENTO. LA TRANSPARENCIA

El concepto de transparencia ya se manejó e incorporó a las respectivas legislaciones en diversos países, antes de la aprobación en nuestro país de la Ley 19/2013. Tras esta ley estatal, en algunas Comunidades Autónomas -por ejemplo, Andalucía[11]- la transparencia está siendo ya objeto de una ley de desarrollo.

Una de los puntos fuertes del RGPD es precisamente la incorporación del principio de transparencia para facilitar la comprensión de las políticas de privacidad e informar adecuadamente sobre el tratamiento de los datos en la UE.

[10] "[…] Dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren […] de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos" (Considerando 78).

[11] Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, Comunidad que fue pionera en este desarrollo. Le siguieron después Murcia, La Rioja, Galicia, Comunidad Foral de Navarra, Cataluña, Aragón, Canarias… En cambio, en la Comunidad de Madrid no existe todavía tal desarrollo, como tampoco en Ceuta.

La transparencia cobra especial relevancia en un mundo digital donde el flujo e intercambio de información es continuo y, con frecuencia, sobre todo en el caso de la publicidad en línea, existe la dificultad de conocer el lugar en el que las páginas webs ubican los datos de los usuarios, así como de saber por quién y con qué finalidad se están recogiendo esos datos (Considerando 58 RGPD). La transparencia permitirá que las personas estén debidamente informadas en este aspecto.

En el ámbito laboral, el principio de transparencia en el tratamiento de los datos personales de los trabajadores es también objeto de atención y cuidado por parte del RGPD en su art. 88, 2.

Por su parte, el art. 5 del RGPD -y parcialmente el Considerando 39- contiene la lista de principios a tener en cuenta en el tratamiento de datos personales (licitud, lealtad, transparencia, exactitud, responsabilidad proactiva, integridad y confidencialidad, junto a la limitación de la finalidad, minimización de datos y limitación del plazo de conservación); algunos de estos principios ya estaban previstos en la LOPD y, previamente, en la Directiva 95/46 (art. 6 a), como la licitud y la lealtad, pero, como se acaba de subrayar, se añade la transparencia: "los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado".

La LOPD ya prohibía expresamente en su art. 4, 7 la recogida de datos por medios fraudulentos, desleales o ilícitos. Mientras la licitud del tratamiento se contempla en el art. 6 RGPD, el principio de transparencia incorporado por el art. 5 del RGPD debe ponerse en relación con el art. 12 del RGPD, en el que se exige al responsable el deber de facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso (San José i Amat, 2017). En definitiva, la importancia del principio de transparencia en un mundo digital radica en "la manera en que se cumplen las obligaciones que recaen sobre el responsable" (Hernández Corchete, 2016: 207) de informar (arts. 13 y 14 RGPD) y comunicar (arts. 15 a 22 y 34 del RGPD) adecuadamente al interesado sobre el tratamiento de sus datos:

"Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados […]. El principio de transparencia se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener

confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento" (Considerando 39 RGPD).

4. TRANSPARENCIA Y EJERCICIO DE LOS DERECHOS

El RGPD crea nuevos derechos, tales como, la portabilidad de datos, el reconocimiento de los derechos de los niños o menores y el derecho a la limitación del tratamiento. Todos ellos se apoyan sobre el principio de información y transparencia que, una vez más, recae sobre el responsable del tratamiento.

Así, el Reglamento regula tanto las características del suministro de la información, por parte del responsable, al interesado (concisión, transparencia e inteligibilidad), como lo relativo a la satisfacción de los derechos.

A las características citadas se suma que la información debe suministrarse por escrito, medios electrónicos o, incluso, verbalmente "siempre que se demuestre la identidad del interesado por otros medios" (art. 12, 1 RGPD) o "en combinación" con iconos normalizados -universalmente identificables- que "deberán ser legibles mecánicamente" (art. 12, 7 RGPD), lo que puede plantear serias dudas de interpretación (López Calvo, 2017: 189)[12], "no sólo sobre el alcance de los iconos, sino también sobre la virtualidad de la <<lectura electrónica>> de una información […]". Sin duda, los iconos, como elementos de representación gráfica, pueden facilitar la comprensión de los elementos que acompañan al tratamiento, pero no ser sustitutos de otros medios, sino complemento de los mismos.

En este sentido, y cuando lo datos se obtengan de redes de comunicaciones, el acceso sencillo a las políticas de privacidad será de gran ayuda. En definitiva, el RGPD "no impone" una forma concreta para proporcionar la información; tan sólo advierte (art. 24. 1) que el responsable, además de garantizar que el tratamiento es conforme con el presente Reglamento, ha de poder demostrarlo (Hernández Corchete, 2016: 210), utilizando las medidas técnicas y organizativas apropiadas. La Directiva 95/46 no especificaba el modo en que debía suministrase la información al interesado, pero la LOPD sí destacó que éste debía ser informado "de modo expreso, preciso e inequívoco" (art. 5 de la misma).

"En cualquier caso, la información proporcionada debe ser suficiente para garantizar que las personas puedan tomar decisiones sobre el tratamiento de sus datos personales. La necesidad de consentimiento para estar informado se traduce en dos requisitos adicionales; en primer lugar, la forma en que se suministra la

[12] La utilización de los iconos normalizados ha sido también objeto de estudio por el Grupo del Artículo 29.

información debe garantizar el uso de un lenguaje apropiado para que los interesados comprendan, con el mayor rigor, [a qué están dando su consentimiento…]; el uso de jerga legal o técnica demasiado complicada no cumpliría con los requisitos de la ley. En segundo lugar, la información proporcionada [directamente a las personas[13]] debe ser clara y suficientemente visible para que [no pase inadvertida]". Esto último, presenta alguna excepción, como es el caso de la grabación de imágenes donde se visualicen un grupo de personas indeterminadas con fines de vigilancia, sobre lo que ya ha habido jurisprudencia relevante[14]. Este punto presenta numerosas aristas y, en estos momentos, excede de nuestro estudio.

En cuanto al ejercicio de los derechos, el responsable del tratamiento facilitará -a título gratuito-[15] al interesado el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición… (arts. 15 a 22 RGPD); para ello, tiene que haber confirmado su identidad[16], pues el responsable puede tener dudas razonables sobre la identidad de la persona, en cuyo caso podrá solicitar la información adicional necesaria. Además, deberá facilitarle información relativa a sus actuaciones sobre la base de una solicitud[17] en el plazo de un mes, ampliable a dos más en casos complejos y teniendo en cuenta el número de solicitudes, debiendo el responsable indicar los motivos de la dilación, debiendo soportar también la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Asimismo, en caso de no dar curso a la solicitud, el responsable deberá informar lo antes posible, y a más tardar en el plazo de un mes, al interesado de las razones de

[13] No es suficiente que la información esté simplemente disponible en algún sitio. Esta ha sido una traducción un poco libre del Dictamen 15/2011, procedente del Grupo de Trabajo sobre Protección de Datos del Art. 29, sobre la definición del consentimiento, citada de una forma soberbia por (Hernández Corchete, 2016: 208-209). Este Dictamen fue adoptado el 3 de julio de 2011 (WP 187) y en él se recogen las condiciones para que ese consentimiento sea válido con arreglo al Derecho de la UE. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp187_en.pdf . [Fecha de consulta: 10.11.2017].

[14] Por supuesto, existen, para contrarrestar, otras limitaciones, tales como no utilizar esas imágenes para otros fines o respetar los períodos de conservación de las grabaciones. Véanse STC 29/2013, de 11 febrero, STC 39/2016, de 3 marzo, STS 77/2017, de 31 enero, en lo que se refiere a España. En la UE, fue interesante la sentencia del TJUE de 11 de diciembre de 2014 (Asunto C-212/13 (František Ryneš / Úřad pro ochranu osobních údajů), planteada por el *Nejvyšší správní soud* -Tribunal Administrativo Supremo- (República Checa).

[15] Sólo cuando las solicitudes del interesado son manifiestamente infundadas o excesivas, el responsable podrá cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación, pudiendo también negarse a actuar (art. 12, 5 RGPD).

[16] Este inciso debe ponerse en relación con el art. 11, 2 RGPD. Si en los casos en que el tratamiento no requiere identificación el responsable es capaz "de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible".

[17] Si la solicitud se presenta por el interesado por medios electrónicos, la información la facilitará el responsable de igual modo cuando sea posible.

que le han llevado a ello, así como de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales (art. 12, 4 RGPD). Se ha afirmado, y no les falta razón, que estas previsiones, de efecto incierto, denotan la obligación de emitir un tipo de "certificado de acto presunto" como se contemplaba, mientras estuvo vigente, en la Ley 30/1992[18] (López Calvo, 2017: 189), con motivo de los actos administrativos producidos por silencio administrativo.

5. EL PRINCIPIO DE TRANSPARENCIA EN LOS MENORES

Tras lo expuesto, es indudable que el principio de transparencia constituye uno de los pilares que refuerzan el alcance del RGPD, haciendo menciones al mismo, no sólo entre los Derechos del interesado (art. 12, sección 1, Capítulo III RGPD), sino también en otros puntos del citado texto, que se especificarán a continuación.

El ámbito de los Menores es uno de los más delicados en lo que se refiere a la Protección de Datos y no sorprende la especial atención de que ha sido objeto ya desde la Propuesta de Reglamento, no sólo en cuanto a calidad de datos y habilitación para el tratamiento (entre los principios), sino también en la regulación contenida en el artículo 8 del RGPD, que detallaremos más adelante.

En este sentido, la transparencia de la información ha pasado "de ser una obligación a configurarse como un derecho (López Calvo, 2017: 188), lo que nos ha llevado a contemplar con satisfacción la especial referencia que el Reglamento Europeo hace sobre los "niños o menores", al tratar la transparencia de la información, comunicación y modalidades de ejercicio de estos derechos:

"El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los arts. 13 y 14, así como cualquier comunicación con arreglo a los arts. 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios" (art. 12 RGPD). Véase, asimismo, Considerando 39 RGPD.

De este modo, dicho precepto reitera lo ya establecido por el considerando 58: "Dado que los niños merecen una protección específica, cualquier información y

[18] De 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común.

comunicación cuyo tratamiento les afecte debe facilitarse <<en un lenguaje claro y sencillo>> que sea fácil de entender".

En efecto, este precepto se está refiriendo tanto a la información que deberá facilitarse cuando los datos personales se obtienen del interesado como a aquélla que se facilitará cuando los datos no se hayan obtenido de aquél. Asimismo, comprende cualquier comunicación en los distintos ámbitos de los derechos -del interesado- de acceso, rectificación, supresión ("el derecho al olvido"), limitación, portabilidad de los datos y oposición, sin olvidar las decisiones individuales automatizadas, "incluida la elaboración de perfiles, que produzca efectos jurídicos [en el interesado] o le afecte significativamente de modo similar. Por último, engloba algo muy relevante: la comunicación de una violación de la seguridad de los datos.

En este sentido, es muy claro el ya mencionado Considerando 58: "El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web […]".

La especial referencia a los niños en el citado precepto debe interpretarse conforme a lo establecido en el art. 8 RGPD - en relación con la oferta directa a niños de servicios de la sociedad de la información-, esto es, cuando tenga como mínimo 16 años y pueda prestar su consentimiento; de otro modo, éste corresponderá o deberá ser autorizado por el titular de la patria potestad o tutela sobre el niño. Bien es verdad que, tratándose del ámbito europeo, los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que ésta no sea inferior a 13 años. El RGPD nos ofrece, así, las condiciones aplicables al consentimiento del menor en relación con los servicios de la Sociedad de la Información.

Se ha considerado que estas normas pueden aplicarse también de forma análoga a otros ámbitos directamente relacionados con los niños, tales como el tratamiento de datos para disposiciones testamentarias, de salud o de ideología, religión y creencia de los menores (Díaz Díaz, 2016).

Todas estas precisiones encuentran su razón de ser en las comprometidas consecuencias a largo plazo de determinados comportamientos; el niño o el menor puede no ser consciente de la magnitud y operatividad de un tratamiento, pudiendo mostrar una despreocupación, y hasta pasar inadvertidas dichas consecuencias. En definitiva, "la transparencia en este caso implica, más que dar

más o mejor información, el logro de un objetivo educativo y de tutela" (Hernández Corchete, 2016: 212).

No en vano, el RGPD, dedica su Considerando 38, a este sector de la sociedad que merece una protección específica de sus datos personales, "ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

En lo que concierne a los derechos de rectificación y olvido, son particularmente pertinentes "si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño […]" (Considerando 65 RGPD).

Es evidente que el tratamiento de datos puede suponer riegos para los derechos y libertades de las personas físicas, pudiendo provocar daños y perjuicios de distinta índole, en particular, en los casos en los que se traten datos personales de "personas vulnerables", como son los niños[19].

Y en lo que concierne al ámbito de los Códigos éticos o de conducta[20] tan necesarios en un mundo digital, al estar destinados a la correcta aplicación del

[19] Así, el Considerando 75 refleja, con exquisito detalle, los distintos supuestos.

[20] Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de estos códigos de conducta; las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento […] (art. 40, 2 RGPD). A tal fin, y junto al supuesto tan delicado de la información proporcionada a los menores, contempla los siguientes:

- el tratamiento leal y transparente;
- los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- la recogida de datos personales;
- la seudonimización de datos personales;
- la información proporcionada al público y a los interesados;
- el ejercicio de los derechos de los interesados;
- las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
- la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

RGPD, éste ha tenido en cuenta las especiales características de los distintos sectores de tratamiento; entre ellos, destaca la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño [art. 40, 2 g) RGPD].

Por último, las denominadas "autoridades de control" -independientes- establecidas en cada Estado miembro[21] para supervisar la aplicación del RGPD y proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento, así como facilitar la libre circulación de datos personales en la Unión, tendrán asignadas diversas funciones, entre las que destaca, la de "promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento; las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención" [art. 57, 1 b) RGPD].

6. ALGUNAS REFLEXIONES Y PERSPECTIVAS DE FUTURO

Se ha dicho que "los datos son el petróleo del siglo XXI"; en este contexto, decidir sobre el uso de las informaciones que le conciernen a la persona (derecho de autodeterminación) exige una importante garantía: "prohibición salvo habilitación"; sin esta base jurídica habilitante[22], el tratamiento será ilegítimo. El principio de minimización debe estar presente también en todos los tratamientos de datos: sólo los mínimos necesarios y por el tiempo preciso. Todo ello se ha traducido en la imposición de nuevas obligaciones para los encargados y responsables de los tratamientos, los cuales van a tener que actuar con una diligencia extrema a la hora de ajustar los tratamientos a los requerimientos legales.

El RGPD, como nueva normativa europea directamente aplicable, va a suponer un auténtico reto para todos ellos, pues estamos hablando de un continuo intercambio

- la transferencia de datos personales a terceros países u organizaciones internacionales, o
- los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

[21] "Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:
— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros" (art. 53, 1 RGPD).

[22] Recordamos, aquí, las tres bases habilitantes: el consentimiento del afectado, la habilitación legal y un interés legítimo prevalente.

de información entre los Estados. La inclusión de la idea de transparencia constituye una de las principales novedades de aquél.

Este incesante flujo de información junto con los mencionados avances tecnológicos ha conducido a utilizar herramientas para analizar grandes volúmenes de datos (*Big Data*), lo que permite realizar peligrosas predicciones. Se ha llegado a afirmar que caminamos hacia "la dictadura de los algoritmos". Esta situación obliga a plantearse un reforzamiento de los derechos de la ciudadanía europea, cuidando al mismo tiempo la vertiente ética. En esta empresa está jugando un papel determinante el TJUE y el Parlamento Europeo.

Se ha subrayado al comienzo que los avances tecnológicos reportan grades ventajas, pero también potenciales riesgos y peligros para los derechos y libertades de las personas físicas, "de gravedad y probabilidad variables" que pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, de los que realiza una minuciosa enumeración el Considerando 75 RGPD.

Recordemos que en la difícil ponderación entre transparencia y protección de datos tuvo grandes repercusiones el caso Wikileaks[23] -fuga de información- a escala planetaria; al analizar las dinámicas de las bases de datos se observa que las oportunidades tecnológicas hacen mucho más sencillo el proceso de recogida, conservación y difusión de los datos personales; al mismo tiempo, la funcionalidad de las grandes bases de datos de tipo social exige accesibilidad y conexión, acceso y compartición. Todo ello, provoca un crecimiento de la vulnerabilidad social que puede derivar en la necesidad de "no revelar todo" en las relaciones personales e institucionales.

En efecto, el derecho de acceso y el derecho de protección de datos inciden sobre informaciones públicas que contienen datos de carácter personal, si bien sus respectivos campos de acción se sitúan en polos opuestos, hasta el punto que se han considerado derechos antagónicos. Conseguir ese difícil equilibrio entre la transparencia y la protección de datos es lo que ha llevado a la doctrina[24] a buscar la idea de "ponderación" que ya destacó Stefano Rodotà[25], el cual ha sido, y sigue

[23] Organización mediática internacional que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público. Cfr. Rodotá, S., 2014. "Las lecciones de Wikileaks: nueva transparencia y nueva distribución del poder" en: Piñar Mañas, J.L. (Dir.), *Transparencia, acceso a la información y protección de datos*. Reus, Madrid, pp. 9 y ss.

[24] Como Director del Consejo de Transparencia y Protección de Datos de Andalucía, así lo puso de relieve Manuel Medina Guerrero, "PROTECCIÓN DE DATOS ¿Es un derecho autónomo? / Intimidad personal y familiar / Transparencia / Nuevas Tecnologías". En *Retos y desafíos del Estado español en el siglo XXI*, IV Ciclo de Seminarios, 13 de diciembre de 2017, Universidad Autónoma de Madrid. Las conclusiones allí planteadas han ayudado en estas reflexiones finales.

[25] Véase nota 23 del presente trabajo.

siendo, referente obligado en materia de protección de datos; es necesario, entonces, argumentar de una forma adecuada y atender a todas las circunstancias concurrentes en cada caso que se plantea.

Esta ponderación ha sido ya tenida en cuenta por el RGPD, al establecer que "los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento"; del mismo modo, "los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios", sin olvidar que "las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento" (Considerando 39). Aquí es donde se encuentra la clave del éxito del principio de transparencia.

A tal fin, el propio RGPD insiste en que "debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados [conocer, de un modo sencillo y automatizado,] y evaluar, con mayor rapidez, el nivel de protección de datos de los productos y servicios correspondientes"[26].

La dimensión global de la transparencia ya llegó; el nuevo marco normativo institucional, nacional e internacional en materia de transparencia y el creciente flujo de datos personales ha provocado un alto grado de inseguridad; dado que la transparencia pública es necesaria, confiemos en que el RGPD permita, en el marco de la UE, superar la escasa capacidad, y a veces poca conciencia, de los Estados frente a lo que se ha venido llamando "tsunami digital".

BIBLIOGRAFÍA

- Carrera Mariscal, A., 2016. "El RGPD: el nuevo Reglamento europeo sobre la protección de datos personales basado en el principio de Accountability". En *The privacy advisor*, 28 de julio de 2016. https://iapp.org/news/a/el-rgpd-el-nuevo-reglamento-europeo-sobre-la-proteccion-de-datos-personales-basado-en-el-principio-de-accountability/ [Fecha de consulta: 15/11/2017].

[26] Considerando 100. Estos sellos o marcas van a permitir al responsable del tratamiento acreditar si facilita al interesado, con la suficiente transparencia, todas las informaciones y comunicaciones que establece el RGPD, si bien, no acaba ahí su responsabilidad, como se ha destacado en páginas anteriores.

- Cotino Hueso, L., 2017. "El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental". En *Teoría y Realidad Constitucional* núm. 40, UNED, pp. 279-316.

- Díaz Díaz, E., 2016. *El nuevo Reglamento General de Protección de los Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*, 18 de abril de 2016. http://www.lawyerpress.com/news/2016_04/1804_16_014.html [Fecha de consulta: 10/11/2017].

- Hernández Corchete, J. A., 2016. "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", en: Piñar Mañas, J.L. (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo de privacidad*. Reus, Madrid, pp. 205-226.

- López Aguilar, J. F., 2017. "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU". En *Teoría y Realidad Constitucional,* núm, 39. UNED, pp. 557-581.

- López Calvo, J., 2017. *Comentarios al Reglamento Europeo de Protección de Datos*. Sepín. Madrid.

- Rallo Lombarte, A. (Ed.), 2014. *El derecho al olvido en Internet. Google versus España*. Centro de Estudios Políticos y Constitucionales. Madrid.

- Rodotá, S., 2014. "Las lecciones de Wikileaks: nueva transparencia y nueva distribución del poder" en: Piñar Mañas, J.L., (Dir.), *Transparencia, acceso a la información y protección de datos*. Reus, Madrid, pp. 9-17.

- San José i Amat, C., 2017. "Los principios del Reglamento (UE) General de Protección de Datos (1)". En *Factor GDA*, 7 de marzo de 2017. https://esaged.wordpress.com/2017/03/07/los-principios-del-reglamento-ue-general-de-proteccion-de-datos-1/ [Fecha de consulta: 05/11/2017].