Anuario Jurídico y Económico Escurialense, **LV (2022) 67-90 / ISSN: 1133-3677**

El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas

The principle of proactive responsibility or accountability as introduce of the legal regime of personal data protection

Dr. Manuel ESTEPA MONTERO
Universidad Complutense de Madrid
mestepa@ucm.es

Resumen: El Reglamento UE 2016/647, del Parlamento y del Consejo, de 27 de abril de 2016, introduce un cambio decisivo en el marco normativo regulador relativo a la protección de las personas físicas en lo que respecta a la protección de datos personales y a la libre circulación de estos datos. Se cambia una normativa que presupone la buena gestión del titular del tratamiento de datos por una nueva regulación que introduce la exigencia de demostrar la necesaria y adecuada implicación del responsable del tratamiento en cada supuesto que sea objeto de examen por la Autoridad independiente de control o, ulteriormente, por las Instancias jurisdiccionales.

Abstract: The EU Regulation 2016/647, of the Parliament and the Council, on April 27th 2016, introduces a decisive change in the regulatory framework relating to the protection of natural persons with regard to the protection of personal data and the free movement of such data. A regulation whose effectiveness is based on the application of it that presupposes the good management of the data controller is changed by a new regulation that introduces the requirement to demonstrate the necessary and adequate involvement of the data controller in each case that is subject to examination by the Independent authority of control or, subsequently, by the Judicial authorities.

Palabras clave: principio de responsabilidad proactiva, protección de datos personales, reglamento general de protección de datos, derechos fundamentales.

Keywords: principle of proactive responsibility or accountability, protection of personal data, general data protection regulation, fundamental rights.

Sumario:

Recibido: agosto 2021.
Aceptado: octubre 2021.

I. INTRODUCCIÓN

La magnitud del daño que para el ámbito de la privacidad puede conllevar un manejo inadecuado de los datos personales en la sociedad digital y de la información en la que nos movemos resulta, ya en sí mismo, lo suficientemente elocuente como para exigir que todo uso sistemático de datos personales se realice con las necesarias garantías para el afectado. El desafío, lejos de aminorarse, no ha hecho más que multiplicarse exponencialmente dado que los flujos de información entre corporaciones y con particulares, de entes públicos con los ciudadanos resulta en nuestros días abrumador. Y lo que es más significativo, existe una tendencia constante hacia la digitalización y trasmisión telemática de datos a través de redes. De manera que, en un futuro próximo, la práctica totalidad de la información relevante se transferirá por este medio; razón por la cuál interesa sobremanera saber cómo se deben gestionar los datos ajenos para no atentar contra los derechos de las personas a decidir, en cada momento de su vida, quién, cómo y para qué realiza un tratamiento de sus datos personales.

Vislumbrando el alcance del problema que suponía el rápido avance tecnológico en un mundo cada vez más globalizado, ya en el año 1980, la OCDE decidió introducir el principio de responsabilidad proactiva o accountabiliy en los Códigos de Conducta o Guías de Protección de la Privacidad y Flujo Transfronterizo de Datos. Por su parte, el Consejo de Europa publicó, en el año 1981, el Convenio 108 mediante el cual fijó una serie de directrices para garantizar, en cada uno de los Estados miembros, el respeto de los derechos y libertades fundamentales de las personas físicas, cualquiera que fuera su nacionalidad o lugar de residencia, en su proyección en la vida privada en relación con el tratamiento automatizado de los datos de carácter personal. El referido Convenio tendría como traducción en España la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos 5/1992, de 29 de octubre (LORTAD), como primera regulación en la materia que atribuyó a las Administraciones públicas las potestades de control, inspección y sanción necesarias para un adecuado desarrollo de las actividades gestoras, públicas o privadas, en el tratamiento de ficheros de datos.

En pleno desarrollo de la normativa sobre protección de datos, el grupo de trabajo europeo consultivo e independiente que se ha ocupado de analizar las cuestiones relativas a la privacidad y la protección de datos personales -el GT Art 29[1]- aprobó, en 2010, un Informe en el que propugnaba la incorporación del aludido principio a la normativa sobre protección de datos; de manera que se garantizara que fueran los responsables del tratamiento de datos personales los que acreditaran ante las respectivas autoridades de control que habían tomado las decisiones apropiadas y eficaces para garantizar los derechos a la protección de sus datos personales.

Tras la primera normativa de alcance europeo que supuso la Directiva 45/1996/CE, de 24 de octubre, que conllevó un cambio en todas las legislaciones de los Estados miembros, dando lugar en España a la aprobación de la LOPD de 13 de diciembre de 1999, las Instituciones Europeas optaron por configurar un cuadro normativo más completo y exigente para asegurar la protección de las personas físicas en relación con el tratamiento de sus datos personales. La idea, finalmente, se concretó en el Reglamento General de Protección de Datos 647/2016/UE, de 27 de abril, del Parlamento Europeo y del Consejo (RGPD)[2], que entró en vigor en España el 25 de mayo de 2018, derogando la ya citada Directiva 95/46/CE. Estamos pues ante una norma obligatoria en todos sus elementos; que goza de los efectos de aplicación directa y preferente en cada Estado parte; y que, además, preveía un amplio periodo de "*vacatio legis*" que permitiría a los destinatarios de sus disposiciones la adopción de las medidas necesarias para su adecuado cumplimiento.

Pues bien, el Reglamento 2016/647 coincide con la Directiva 95/46/CE en la definición de los dos objetivos nucleares a garantizar: que el tratamiento de los datos personales no vulnere los derechos fundamentales y que, al mismo tiempo, se asegure la libre circulación de los datos entre los Estados miembros. En efecto, se trata de proteger "*los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*" (art.1.2 del Reglamento UE 2016/679). El RGPD, por lo tanto, parte de la

[1] El Grupo de Trabajo del artículo 29 se constituyó en el año 1996 como consecuencia de la entrada en vigor de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas y la libre circulación de estos datos. Se encuentra integrado por representantes de todas las Autoridades de control de los Estados integrantes de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea. En 2010, aprueba la opinión 3/2010 en la que propugna la incorporación del principio de responsabilidad proactiva a la normativa de los Estados miembros de la UE en materia de protección de datos.

[2] El título del Reglamento Europeo coincide, y no por casualidad, con el de la Directiva de 1995 al proyectarse sobre la protección de datos de las personas físicas y de libre circulación de estos datos.

concepción del derecho a la protección de datos como derecho fundamental; como resalta su Considerando 1°, siguiendo en este punto lo dispuesto en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) que establecen que "*toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*". Se pretende contribuir a la consecución de un espacio de libertad, seguridad y justicia, al mismo tiempo que se avanza en la unión económica, así como en el progreso económico y social que permita mejorar el bienestar de los ciudadanos. El tratamiento de datos personales debe servir a la humanidad, razón por la cual, ha de respetar el derecho a la autodeterminación personal en su manejo; la intimidad personal y familiar (Considerando 4º RGPD). Pero, simultáneamente, el nuevo Reglamento se orienta hacia el fomento de "*la libre circulación de los datos personales en la Unión*", de modo que "*no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*" (art.1.3 del Reglamento UE 2016/679). En consecuencia, la protección de datos personales no constituye un derecho absoluto, sino que debe armonizarse con el respeto a otros derechos fundamentales y libertades, como la libertad de empresa, teniendo presente el principio de proporcionalidad.

II. LA RESPONSABILIDAD PROACTIVA O ACCOUNTABILITY EN EL CONTEXTO DE LA NUEVA NORMATIVA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

2.1. *El principio de responsabilidad proactiva en el marco del RGPD*

Como afirma la Ley Orgánica de Protección de Datos Personales y Derechos Digitales, de 5 de diciembre de 2018 (en adelante, LOPDDG), en su Preámbulo, el RGPD supone la revisión de las bases legales del modelo europeo de protección de datos, más allá de una mera actualización de la normativa vigente. Aunque, como ha recalcado la Comisión Europea, mantiene los conceptos y principios básicos de la legislación en materia de protección de datos establecida en 1995[3]. El nuevo Reglamento europeo, por lo tanto, sí que introdujo cambios relevantes respecto de la regulación previa, tanto más importantes en cuanto que su incorporación a una norma de aplicación directa, como es el Reglamento, les dota de un carácter homogéneo en la medida que su interpretación jurídica

[3] Comunicación COM (2018) 43, pp. 10. "Es fundamental que los operadores dispongan de un conjunto de orientaciones único y coherente, las directrices actuales a nivel nacional deben derogarse o adaptarse a la adoptadas por el Grupo de Trabajo del artículo 29 o el Comité Europeo de Protección de Datos sobre el mismo tema".

completa descansa en la doctrina del TJUE. Destacan en este sentido, por ejemplo, la definición y regulación del consentimiento (arts. 4 y 7), la regulación del derecho al olvido y a la portabilidad (arts. 17 y 20), los principios de privacidad desde el diseño y por defecto (art. 25), la nueva figura del delegado de protección de datos (arts. 37 y 39) o la necesidad de evaluación del impacto que supone el tratamiento de datos personales y la necesidad de consulta con la Autoridad de control (arts. 35 y 36).

Entre las novedades del nuevo texto, destaca sobremanera, a los efectos de garantizar su cumplimiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento; así como el riesgo para los derechos y libertades de las personas, el principio de responsabilidad proactiva, recogido en sus artículos 5.2 y 24.1, que podría ser definido como la exigencia de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento que realiza es conforme con el Reglamento. Se trata de dar un paso más en el compromiso del responsable de datos con sus obligaciones de protección de datos[4]. Se exige no sólo cumplir la normativa vigente sino encontrarse, en todo momento, en condiciones de demostrar que se ha actuado de modo diligente teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento. Con lo que la implicación de estos responsables con la protección de los datos personales debe ponerse de manifiesto desde el inicio del procedimiento, estando en condiciones de dar cuentas de ello, siempre que sea requerido, por las Autoridades de control y por los ciudadanos interesados.

2.2. *Delimitación conceptual del principio de responsabilidad proactiva o de rendición de cuentas*

Esta actitud proactiva se podría resumir en la frase que ha popularizado la AEPD, según la cual, "*no incumplir ya no será suficiente*"[5]. Se trata de asegurar un compromiso elevado de cumplimiento que permita garantizar el necesario respeto a los derechos de los particulares a la vez que facilita el incremento incesante del flujo de datos que circula entre los entes públicos, las corporaciones y los particulares. A este respecto, puede citarse como un movimiento precedente

[4] PIÑAR MAÑAS, J. L., *Reglamento General de Protección de Datos, Hacia un nuevo modelo de Privacidad*. 1ª edición, Editorial Reus, Madrid, 2016, p. 16, afirma: "Pero el Reglamento introduce, a veces de forma soterrada, un nuevo modelo de protección de datos para Europa. Un modelo que podemos decir que pasa de la gestión de datos al uso responsable de la información. Este es seguramente el más profundo cambio que el Reglamento va a imponer".

[5] GARCÍA HERRERO J., *Responsabilidad Activa (Accountability) en el Reglamento General de Protección de Datos*, Actualidad Jurídica Aranzadi, febrero 2017, p. 28.

al fenómeno examinado, aunque con diferencias sustantivas, aquél que comenzó con la Directiva de servicios en el mercado interior, 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre, en virtud de la cual, con el propósito de fomentar el libre establecimiento y circulación de actividades de servicio en Europa, se pasó de una cultura del control preventivo por los poderes públicos de los requisitos legales a un esquema normativo en el que lo que realmente importa es confirmar, en el momento oportuno, que se cumple materialmente con la normativa exigida. Lo que se concretó en una fuerte restricción del régimen de las autorizaciones previas (arts. 9 a 15), eliminándolas o bien sustituyéndolas por comunicaciones previas o declaraciones responsables. Con lo que el particular carecía ya de la protección jurídica que le otorgaba la licencia de actividad otorgada por la Autoridad competente[6]. Todo ello dentro de una cultura social que enfatiza el aspecto autónomo del comportamiento profesional con miras al crecimiento del mercado interior. Lo anterior porque, en materia de Administración pública y políticas públicas, la referencia, hasta bien entrada la segunda mitad del siglo XX, había estado centrada en la acción del Estado y del Gobierno por cuanto, en la teoría tradicional, a él corresponde la dirección de la sociedad. No obstante, a raíz de la crisis económica y fiscal que asoló Europa y los Estados Unidos de América desde finales de los años 70 del siglo XX, comenzó a plantearse una redefinición del papel del Estado y sobre todo de la actuación de los Gobiernos.

Se estima, por lo tanto, desaconsejable en las nuevas circunstancias, la denominada vieja gobernanza («*old governance*») que concebía al Poder Ejecutivo como agente principal y único o al menos preeminente de la dirección de la sociedad. Dotándolo de abundantes recursos e instituciones coactivas, así como de un nivel destacado de autonomía funcional en la consideración de que la sociedad, por sí misma, resulta ingobernable. Lo que, en cualquier caso, también conforme a las modernas teorías doctrinales, puede llegar a ser cierto en determinadas circunstancias económicas y sociales (v.gr., países con un muy escaso desarrollo económico y social en períodos de inestabilidad). Defendiéndose, frente a este concepto, la nueva gobernación («*new governance*»), que enfatiza los caracteres de recomposición de las capacidades directivas y de integración de los diferentes sujetos económicos y sociales mediante la formación de alianzas o entendimientos que articulan y fortalecen vínculos, la mayoría de las veces, ya preexistentes. Con ello, la acción del Poder Ejecutivo engloba la visión y los intereses de la competencia, mediante la integración de los agentes

[6] Vid. El art. 71 bis de la Ley de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común (LRJAPYPAC), en la redacción dada por el art. 2.3 de la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre el libre acceso a las actividades de servicio y su ejercicio. E igualmente, el vigente art. 69 de la Ley de Procedimiento administrativo Común 30/2015, de 1 de octubre, (LPAC).

económicos y sociales, como la perspectiva y los intereses propios de los grupos que operan en el ámbito de la acción solidaria.

Pues bien, ya en el siglo XXI, nos encontraríamos en un nuevo estadio evolutivo en el que no bastaría con el cumplimiento por los ciudadanos -personas físicas o jurídicas- de unos límites mínimos preestablecidos en la norma sino que, además de su participación colaborativa con los poderes públicos, se les exige un actitud permanente de toma de decisiones orientada al cumplimiento de los objetivos fijados por el Legislador. Esta nueva perspectiva comienza ya a dar uno de sus primeros frutos en el ámbito jurídico con la llamada «*cultura del cumplimiento*» en relación con la determinación de la responsabilidad penal de las corporaciones, de acuerdo con el art. 31 bis del Código Penal, puesto que, aunque no se encuentra recogido en el mismo ni forma parte objetiva del tipo penal, sí constituye un elemento mencionado de manera constante por los operadores jurídicos en el contexto internacional del que se hace eco la Sentencia de la Sección 1ª de la Sala de lo Penal del Tribunal Supremo 154/2016, de 29 de febrero (Ar. 600/2016, F.J. 8º).

En concreto, la referida Resolución judicial considera que la definición de cual ha sido la actuación relevante de la persona jurídica, a efectos de la determinación de su responsabilidad penal (a tenor de lo dispuesto en el art. 31 bis del Código), ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquella ha sido posible o facilitado «*por la carencia de una cultura de respeto al Derecho, como fuente de inspiración de la actuación de su estructura organizativa e independiente de la de cada una de las personas físicas que la integran*». Ética empresarial que habría de manifestarse en alguna clase de formas concretas de vigilancia y control del comportamiento de sus directivos y subordinados jerárquicos, tendentes a la evitación de la comisión por éstos de los delitos enumerados en el Libro II del Código Penal.

Esta cultura de respeto al Derecho debería concretarse en la existencia de modelos organizativos y de administración que cumplan las exigencias concretamente enumeradas en el actual art. 31 bis 2 y 5. De manera que la exoneración se basa en la prueba de la existencia de herramientas de control idóneas y eficaces cuya ausencia integraría, por el contrario, el núcleo típico de la responsabilidad penal de la persona jurídica, complementario de la comisión del ilícito por la persona física. Y es que, a juicio del Alto Tribunal, la presencia de adecuados mecanismos de control lo que supone es la inexistencia misma de la infracción. Circunstancia eximente de responsabilidad que, en definitiva, lo que persigue primordialmente es posibilitar la pronta exoneración de esa responsabilidad

de la persona jurídica, en evitación de mayores daños para la reputación de la entidad.

Por consiguiente, el núcleo de la responsabilidad de la persona jurídica residiría en la inexistencia de las medidas de control adecuadas para la evitación de la comisión de delitos, que hagan patente «*una voluntad seria de reforzar la virtualidad de la norma*», independientemente de aquellos requisitos, más concretados legalmente en forma de las denominadas "compliances" o "modelos de cumplimiento" exigidos para la aplicación de la eximente que, además, ciertas personas jurídicas, por su pequeño tamaño o menor capacidad económica, no pudieran cumplidamente implementar. Debiendo destacarse, a este respecto, como también la Circular de la Fiscalía General del Estado 1/2016, de 22 de enero[7], hizo reiterada mención a expresiones tales como la exigencia de la "cultura ética empresarial" o "cultura corporativa de respeto a la Ley" o "cultura de cumplimiento", como integradoras de los mecanismos de prevención de la comisión de delitos en su seno; constituyendo un elemento decisivo a la hora de establecer la responsabilidad penal de la persona jurídica, independientemente incluso del cumplimiento estricto de los requisitos previstos en el Código Penal.

Como dirá, posteriormente, la Sentencia de la misma Sección 1ª de la Sala Segunda del Tribunal Supremo 123/2019, de 8 de marzo (Ar. 1064/2019, F.J. 1ª). La persona jurídica no es condenada por un (hoy inexistente) delito de omisión de programas de cumplimiento normativo o por la inexistencia de una cultura de respeto al Derecho. Para que sea condenada, se precisa la comisión de uno de los delitos que, previstos en la parte especial del Código Penal, operan como delito antecedente, tal como aparece contemplado en el artículo 31 bis; cometido por una de las personas en dicho precepto mencionadas. La condena recaerá precisamente por ese delito. Siendo necesario esclarecer que las hipotéticas medidas organizativas y de control que pudieran haberse tomado podrían haber evitado su comisión. De manera que a la persona jurídica no se le imputa un delito especial integrado por un comportamiento de tipo omisivo, sino el mismo delito que se imputa a la persona física, en el cual, de ordinario, participará a través de una ausencia de las cautelas obligadas por su posición de garante de la legalidad aplicable, necesarias para impedir la comisión de determinados delitos.

Por consiguiente, existe ya una primera exigencia legal, en el ámbito de penal, de aplicación de la referida «*cultura del cumplimiento*» por parte de

[7] Circular 1/2016 de la Fiscalía General del Estado, *Sobre responsabilidad penal de las personas jurídicas conforme a la reforma el Código Penal efectuada por la Ley Orgánica 1/2015* (Referencia: FIS-C-2016-0001), 2016, pp. 20, 26 y 27, entre otras.

los entes corporativos que promueve una ética empresarial concretada en planes y programas de gestión que implica un cambio de paradigma frente a la exigencia tradicional por el Legislador de mero acatamiento de la ley al construirse como una responsabilidad por comportamiento omisivo que impediría la concurrencia de una eximente de responsabilidad. Y el citado avance jurisprudencial en materia penal se ha visto sintonizado en el tiempo con la aparición, también en 2016, del ya citado principio de responsabilidad proactiva en relación con la protección de datos de carácter personal que promueve no sólo la aplicación de medidas que permitan cumplir la ley sino también de asegurarse que toda la actividad empresarial desarrollada facilite el demostrar que se cumplen adecuadamente la normativa aplicable. Cómo afirma el Considerando 72 del RGPD, la responsabilidad del tratamiento de datos personales realizado por el responsable del tratamiento o por su cuenta constituye un requisito *sine qua non*. Concretándose en la idea de que el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento, incluida la eficacia de las medidas. Por consiguiente, la clave del concepto se sitúa en la capacidad para demostrar la inocencia del responsable del tratamiento, en el sentido que aplicó las medidas precisas y eficaces para que se cumpliera la normativa en vigor. Nos encontramos, por consiguiente, con un concepto que se configura como el eje vertebrador del resto de la regulación de la protección de datos personales, en cuanto noción de carácter horizontal que informa cada uno de los conceptos operativos del régimen jurídico aplicable. Me estoy refiriendo, de modo específico, a la noción de evaluación del riesgo y la conveniencia de que las empresas se doten de sellos de calidad y de códigos de conducta que refuercen esa capacidad de acreditación de diligencia en su actuación. Pero estos aspectos puntuales procedo a analizarlos en los siguientes apartados del presente artículo.

En cualquier caso, resulta importante destacar que nos encontramos ante un concepto de carácter abierto que bien podría identificarse con la definición de «concepto jurídico indeterminado» que, como sabemos, es empleado en las descripciones normativas de los supuestos de hecho (p.ej., urgencia, utilidad pública, orden público, amenaza de peligro, incluso "interés general") abocando a una única solución justa. De manera que, siendo en abstracto indeterminado, resulta sin embargo determinable en atención a las circunstancias del caso concreto. No otra cosa es lo que prescribe el Legislador al exigir medidas oportunas y eficaces. Así junto con las zonas de certeza positiva o negativa, existe una "*zona de incertidumbre o penumbra*" en la que resulta muy difícil discernir si la subsunción del supuesto de hecho en el concepto es factible. Pues bien, es justamente en ese nivel en el que el sujeto responsable de la actividad de que se trata -en el presente caso, el responsable del tratamiento- goza de un margen para decidir. De modo que, en caso de duda sobre el grado de adecuación

y acierto de las medidas tomadas, la Autoridad de Control competente debería eximirle de responsabilidad so pena, en caso contrario, de coartar la necesaria libertad de dirección empresarial. Lo que, en la mayoría de los casos, conlleva una rigidez excesiva en el tratamiento masivo del flujo de información con el consiguiente perjuicio para la actividad del sector privado y para el buen funcionamiento de la sociedad de la información[8].

La necesaria rendición de cuentas se ha de realizar, por consiguiente, en función de las circunstancias en las que se desarrolla el tratamiento de datos objeto de control. Lo que queda meridianamente claro si tenemos en cuenta que ya el propio artículo 24 al igual que el Considerando 74 del RGPD disponen, de manera expresa, como la gestión que se realice deberá tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo de diversa probabilidad y gravedad para los derechos y libertades de las personas. A lo anterior, añade el referido precepto la exigencia de que las medidas que se apliquen sean revisadas y modificadas siempre que las nuevas circunstancias lo hagan necesario. Se trata, al mismo tiempo, de un concepto evolutivo que surge de la necesidad de las sociedades de alcanzar un nivel de eficacia y transparencia en la actividad pública y privada que de garantías de respeto del Ordenamiento jurídico, así como de la necesaria consecución de unos estándares mínimos de calidad[9]. De manera que se configura como un instrumento para la consecución de tales objetivos susceptible de ampliación y profundización en su contenido en función del grado de desarrollo tecnológico y social.

2.3. *El principio de responsabilidad proactiva en la Jurisprudencia del Tribunal de Justicia de la Unión Europea*

El Comité Europeo de Protección de Datos (CEPD) hizo público el 10 de noviembre de 2020 sendas recomendaciones vinculadas con la jurisprudencia sentada por la Gran Sala del el Tribunal de Justicia de la Unión Europea en su Sentencia de 16 de julio de 2020, adoptada en el asunto C-311/18 (*Maximiliam Schrems II*), en las que, esencialmente, consideraba que la Decisión de Ejecución (UE) 2016/1250 (denominada Escudo de Privacidad UE-EE.UU, Decisión EP) aprobada por la Comisión, de 12 de julio de 2016, adoptada con arreglo a

[8] Existe, no obstante, un elemento novedoso en cuanto al control del nuevo principio de la responsabilidad proactiva o accountability que vendría dado por el hecho de que la doctrina jurisdiccional entiende que la correcta aplicación de un concepto jurídico indeterminado se justifica en la razonabilidad de la decisión tomada y no en la oportunidad de la misma (STS de 20 de octubre de 1980). Pero es que en este caso la oportunidad y eficacia de la medida forman parte esencial de la naturaleza jurídica del concepto jurídico que se aplica.

[9] PUYOL MONTERO, J.*, el principio de responsabilidad proactiva*, confilegal, 26 de febrero de 2018, www.confilegal.com, sostiene como: «*en rigor no existe un consenso sobre qué es la rendición de cuentas o "accountability": es un concepto en construcción*».

la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de datos personales, es inválida. Pues vulneraba los derechos fundamentales a la vida privada (art. 7 CDFUE) y a la protección de datos (art. 8 CDFUE) al considerar que la primacía que otorga respecto de las exigencias relativas a la seguridad nacional, el interés público y el cumplimiento de la ley norteamericana, comportaban una disminución de las garantías de la protección de datos personales en la medida en que permitía la aplicación de la normativa interna estadounidense referida a su acceso y utilización por la autoridades de aquel país que no se encuentra confeccionada de acuerdo con exigencias sustancialmente equivalentes a las requeridas en el Derecho de la Unión, sin que tampoco estuviera asegurado el ejercicio del derecho a la tutela judicial efectiva.

La referida Sentencia, adoptada en un procedimiento prejudicial, del art. 267 TFUE, pone de manifiesto como, en relación con la transferencia de datos personales mediante clausulas tipo de protección de datos (art. 46 RGPD), el exportador de datos personales -en el presente caso la Compañía Facebook Ireland Ltd-. debe asegurarse que el país en donde reside el importador -Facebook Inc- ofrece garantías adecuadas de protección equivalentes a las mantenidas en el Espacio Económico Europeo (EEE); así como de que los interesados cuenten «con derechos exigibles y acciones legales efectivas». Pudiendo proporcionarse esas garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión Europea.

El TJUE concluye que la normativa estadounidense no ofrece el mismo nivel de protección al ciudadano de la Unión en cuanto a la posibilidad de investigación por parte de las Autoridades públicas ni tampoco en cuanto al posible ejercicio de acciones legales. Por lo que declara inválida la previa Decisión de la Comisión Europea denominada Escudo de Privacidad EU-EE.UU.

La Recomendación del CEPD 1/2020 expone, desarrollando la doctrina jurisprudencial sentada por el TJUE, que no resulta suficiente con adoptar alguno de los instrumentos que habilita el Reglamento General de Protección de Datos (cláusulas contractuales tipo u otro tipo de instrumento) e incluirlo en el contrato que regula la relación entre las partes involucradas en la trasferencia. Los responsables del tratamiento deben verificar en cada supuesto y, en su caso, en colaboración con el receptor del tercer país, si la legislación o la práctica del tercer país limitan a la eficacia de las garantías apropiadas contenidas en los instrumentos de transferencia del artículo 46 del RGPD. En tales supuestos, el Tribunal deja abierta la posibilidad de que los emisores apliquen medidas complementarias que palíen estas lagunas de protección, a fin de que esta alcance el nivel exigido por el Derecho de la Unión. El Tribunal no expone

qué medidas se podrían adoptar. Sin embargo, el Tribunal recalcan que los emisores tendrán que determinarlas de modo individualizado. Dicha exigencia concuerda con el principio de responsabilidad proactiva del artículo 5, apartado 2, del RGPD*,* que obliga a que los responsables del tratamiento sean responsables y capaces de demostrar el cumplimiento de los principios del RGPD relativos al tratamiento de datos personales. Por lo tanto, el principio de responsabilidad proactiva que rige la protección de datos personales, comporta la exigencia de que el responsable del tratamiento asegure la efectiva privacidad e integridad de los datos. De modo que, en el futuro, las personas jurídicas deben adoptar medidas adecuadas que, en la práctica, proporcionen un nivel de seguridad cuasi pleno; en el sentido de que los datos objeto de la transferencia no se verán afectados en el tercer país ni tampoco con ocasión de ulteriores operaciones de transferencia que el receptor pueda llevar a cabo.

Para ayudar a los exportadores (ya sean responsables o encargados del tratamiento, entidades privadas u organismos públicos que traten datos personales en el ámbito de aplicación del RGPD) con la compleja tarea de evaluar a terceros países y de establecer medidas complementarias adecuadas cuando sea necesario, el Comité Europeo de Protección de Datos (CEPD) facilita, en la citada Recomendación 1/2020, una relación de medidas que conviene seguir. Estas recomendaciones proporcionan a los exportadores una serie de pasos, posibles fuentes de información y algunos ejemplos de medidas complementarias que podrían aplicarse.

Por su parte, la Recomendación 2/2020 del CEPD especifica las garantías esenciales dentro del ámbito de la UE (las *European Essential Guarantees*, "EGG") que han de contener las medidas de vigilancia que se adopten al transferir los datos personales para asegurarse de que las injerencias en los derechos a la intimidad y a la protección de datos personales no exceden de lo necesario y proporcionado en una sociedad democrática basándose en la jurisprudencial del TJUE configurada a raíz de los asuntos Shrems I y II. El objetivo es proporcionar elementos para analizar si tales injerencias, llevadas a cabo principalmente por agencias de seguridad nacional y cuerpos de seguridad del Estado, son justificables. No obstante, aportan igualmente a las empresas medios para verificar si es factible realizar las transferencias de datos hacia terceros Estados.

Pues bien, partiendo del análisis de la citada jurisprudencia del TJUE, CEPD concreta los requisitos jurídicos aplicables para que sean justificables las limitaciones a los derechos a la protección de datos y a la intimidad reconocidos por la Carta, resumiéndolos en cuatro garantías esenciales europeas: El tratamiento se debe basar en normas claras, precisas y accesibles (debiendo además la norma legal ser imperativa en el Derecho interno, según el TJUE). Se tiene que

demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos (ponderando la gravedad de la injerencia y la importancia para el objetivo de interés público perseguido). Asimismo, debe existir un mecanismo de supervisión independiente (por ejemplo, una instancia parlamentaria o judicial, tal y como afirma el TEDH[10]). Y, por último, la idea de que el interesado debe tener a su disposición recursos efectivos que permitan el ejercicio de su derecho a la tutela juridicial efectiva reconocido en el art. 47 CEDFUE, según mantiene el TJUE en la Sentencia Shrems I.

Finalmente, interesa resaltar que existe ya otra Sentencia en la que el TJUE hace igualmente aplicación del principio de responsabilidad proactiva en la protección de datos. Se trata de la Sentencia de la Sala Segunda del TJUE de 11 de noviembre de 2020 (Ar. 268/2020) en el asunto Orange România SA contra Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Per (ANSPDCP). Nos encontramos, en esta ocasión, ante un supuesto de exclusión material del consentimiento del cliente en la medida en que los contratos del proveedor de servicios de telecomunicaciones móviles, si bien contienen una cláusula conforme a la cual los clientes interesados han sido informados y han dado su consentimiento, lo cierto era que la casilla relativa a dicha cláusula ya había sido marcada por los agentes comerciales antes de que esos clientes comerciales procedieran a la firma, obteniendo y conservando copias de documentos de identidad de esos clientes con fines de identificación.

El TJUE entiende que los artículos 2.h), y 7.a) , de la Directiva 95/46/CE y los artículos 4.11, y 6.1.a) del Reglamento 2016/679 deben interpretarse en el sentido de que corresponde al responsable del tratamiento de los datos demostrar que el interesado ha manifestado su consentimiento para el tratamiento de sus datos personales *mediante un comportamiento activo* y que ha recibido, previamente, información respecto de todas las circunstancias relacionadas con ese tratamiento, con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, que le permita determinar sin dificultad

[10] Sentencia del Tribunal Europeo de Derechos Humanos (TEDH), de 6 de septiembre de 1978, asunto Klass y otros vs República Federal Alemana, apartados 21, 53 y 67 (Ar. 1/1978). La Sentencia constata que, en la RFA, se cumple con la exigencias, del art. 8.2 CEDH, de que toda injerencia del poder público en el «*derecho a la vida privada y familiar, al domicilio y a la correspondencia*» se encuentre prevista en la ley y sea necesaria en una sociedad democrática,; concretándose dicha exigencia, para el caso analizado, en que toda restricción del secreto de la correspondencia postal y de las comunicaciones telefónicas se encuentre sometida a un control independiente (en la RFA: el Comité de 5 parlamentarios y la Comisión G10, nombrada por aquél, compuesta por un Presidente apto para acceder a las magistratura y dos vocales asesores); así como en que el interesado, que sea notificado a posteriori de la injerencia practicada, tenga la posibilidad de presentar un recurso, aunque no necesariamente judicial (en el caso alemán, ante el G10 y posteriormente ante el Tribunal Constitucional Federal).

las consecuencias de dicho consentimiento, de modo que se garantice que éste se otorga con pleno conocimiento de causa. Sin que pueda cumplir tales exigencias un contrato como el señalado o en el que las estipulaciones contractuales de dicho contrato puedan inducir al interesado a error sobre la posibilidad de celebrar el contrato en cuestión pese a negarse a consentir en el tratamiento de sus datos; o cuando la libre elección de oponerse a dicha obtención y dicha conservación se vea indebidamente obstaculizada por ese responsable, al exigir que el interesado, para negarse a dar su consentimiento, cumplimente un formulario adicional en el que haga constar esa negativa.

III. LA GESTIÓN DEL RIESGO COMO ELEMENTO DECISIVO EN LA APLICABILIDAD DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El principio de responsabilidad proactiva tiene como presupuesto clave el que el responsable del tratamiento se encuentre en disposición, desde el inicio del procedimiento del manejo de datos, de demostrar que ha tenido una actitud diligente en cada uno de los pasos a seguir ya sea tomando decisiones o gestionando las mismas. Se trata de estar en condiciones de probar la inocencia ante los eventuales afectados, las Autoridades de Control y, en su caso, ante las instancias jurisdiccionales Sin embargo, resulta especialmente interesante considerar el que dicha capacidad de prueba del responsable se sustenta, a su vez, en un concepto cada vez más empleado en cuanto ligado al funcionamiento de sistemas en entornos complejos, como es el caso de la autorización de operaciones de vuelo: me estoy refiriendo a la gestión del riesgo inherente a la puesta en marcha de una operación de protección de datos en atención a las circunstancias relevantes que concurran al tiempo de su realización. A este respecto, interesa resaltar que el RGPD contempla una serie de niveles de gestión del riesgo que van desde una situación de normalidad -no exenta de peligro- hasta escenarios en los que, junto a niveles elevados de probabilidad de daños y perjuicios, se torna difícil la toma de decisiones por no estar claro cuál es la mejor alternativa a tomar y cuál puede ser el alcance de que los potenciales efectos negativos lleguen a concretarse.

El primer nivel, de normalidad, vendría dado por la previsión contenida en el artículo 32 RGPD, y completada por el Considerando 78, conforme al cual, se prevé todo un repertorio de medidas técnicas y organizativas posibles a adoptar por el responsable del tratamiento que se han de ajustar al supuesto concreto en atención a una serie de variables, en parte ya enunciadas en el art. 24 RGPD (la naturaleza, el ámbito, el contexto y los fines del tratamiento, y los riesgos de diversa probabilidad y gravedad para los derechos y libertades

de las personas físicas). Pero, en todo caso, la proximidad de sufrir un daño debe estimarse mediante un análisis objetivo que permita determinar si las operaciones de tratamiento de datos suponen un riesgo y si el mismo es alto (Considerando 76). De modo específico, el precepto cita como factores adicionales a considerar para evaluar el cuadro de medidas a adoptar, el estado de la técnica y los costes de aplicación de las medidas que se tomen lo que, en parte, constituye una obviedad pero que no deja de tener trascendencia a la hora de examinar una posible reclamación de responsabilidad patrimonial en orden a acotar el grado de diligencia que le era exigible al titular del tratamiento.

Con carácter básico, el Legislador europeo propugna como medidas técnicas y organizativas de garantía : a) Disminuir al máximo el tiempo del tratamiento; b) la seudonimización y el cifrado de datos personales; c) asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; d) la posibilidad de recuperar la disponibilidad y el acceso a los datos personales en un corto plazo de tiempo en caso de incidente físico o técnico; y, por último, e) la adopción de procedimientos periódicos de supervisión, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Salvo la primera de las medidas que no está incorporada al precepto y, por lo tanto, tiene una naturaleza meramente orientativa, nos encontramos ante una serie de proposiciones abstractas que ponen el acento en cualidades propias de los sistemas de tratamiento y transmisión de datos más avanzados; cuando no en la disponibilidad de un equipo humano experto que sea capaz de gestionar en tiempo real y de manera continuada el diseño, gestión y conservación de los datos. Es más, entre las propuestas que lleva a cabo el Considerando 78, se formula una dirigida a los productores de los productos, servicios y aplicaciones en el sentido de que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Idea que por sí misma, si no va acompañada de ninguna previsión normativa específica que la haga obligada, no deja de ser un buen deseo del Legislador. Con lo que la responsabilidad desde el diseño y por defecto seguirá recayendo, como hasta ahora, en el responsable del tratamiento (art. 25.1 y 2 RGPD); por cuanto es en este nivel en el que se residencia la aplicación de la vigente normativa de protección de datos. La privacidad debe estar integrada en toda la arquitectura tecnológica pero, aun dando por supuesto que los productores de productos, servicios y aplicaciones asumen la filosofía expuesta del RGPD, es el diseño que esboza el titular del tratamiento el que se verá sometido a examen.

Un segundo nivel de riesgo al que ha de atender el titular del tratamiento de datos personales viene constituido por las denominadas «*evaluaciones de impacto relativas a la protección de datos*». En este supuesto, nos encontramos ante operaciones de alto riesgo en las que el Legislador europeo revela su preocupación por reducir al mínimo la posibilidad de que se deriven daños y perjuicios debido a la naturaleza de las operaciones que se van a acometer. Se trata de supuestos extremadamente sensibles por la gravedad de las repercusiones que pueden derivarse para la integridad de los derechos y libertades de las personas físicas afectadas. Evaluación sistemática y exhaustiva de aspectos personales; tratamiento a gran escala de categorías especiales de datos, como los relativos a la salud; elaboración de perfiles en base a los cuales se tomen decisiones con efectos jurídicos y que tenga un efecto sensible en la vida de las personas; manejo de datos que revelen el origen étnico, la ideología, religión o la salud de las personas (art. 34 RGPD). El art. 28.2 LOPDDG, por su parte, identifica una serie de supuestos en los que existe una posibilidad de que el riesgo se incremente y que se añaden a los ya previstos en el art. 34.2 RGPD. De manera que, dada la trascendencia de las operaciones a realizar, se obliga al titular del tratamiento a realizar un análisis sistemático del proceso a desarrollar que se concretará en la denominada «evaluación de impacto». Un documento que obliga al responsable del tratamiento a exponer de manera razonada y sistemática el conjunto de elementos de garantía que va a aplicar en atención a los riesgos detectados en el supuesto o supuestos concretos que se contemplan. El artículo 35.7 RGPD expone el contenido mínimo del documento de evaluación de impacto que, como es obvio, alcanzará una descripción completa de las operaciones de tratamiento a realizar y de los fines que se persiguen; la necesidad y proporcionalidad del procedimiento para alcanzar los fines señalados; la prospectiva de los posibles daños y perjuicios; así como las medidas que se prevén para garantizar los derechos y libertades de las personas y su conformidad con el Reglamento.

Estamos pues ante una actuación compleja respecto de la que, por lo mismo, el titular del tratamiento debe estar asistido por personal experto en la materia. Y es por esta razón por la que el RGPD obliga a que, en el caso de que exista, el responsable del tratamiento acuda obligatoriamente a los conocimientos y experiencias del Delegado de protección de datos. Nos encontramos ante una nueva figura, recogida en el artículo 37 RGPD y el art. 34 y siguientes LOPDDG, creada específicamente para asegurar la máxima protección de datos en supuestos de tratamientos sistemáticos y a gran escala de datos de especial trascendencia relativos a los poderes públicos, de carácter judicial, datos especialmente sensibles previstos en el art. 9 RGPD. Razón por la cual resulta lógico que sobre el mismo resida materialmente el encargo de confeccionar una correcta evaluación de impacto de las operaciones propuestas. A él compete la adopción de medidas de cumplimiento normativo, de supervisión y garantía. Asesora de modo continuo

al responsable y al encargado de protección de datos del ente o corporación en el que trabaje; labor que se extiende a los subcontratistas. Atiende asimismo las reclamaciones por razón de daños que reciba la corporación aunque no asume la responsabilidad de las acciones ejecutadas por el organismo o entidad a la que sirve. Y actúa como enlace con las Autoridades de control competentes, función ésta última que resulta decisiva en el tercero de los niveles de contemplación del riesgo que prevé el RGPD.

Me refiero, de modo específico, a la previsión que contiene la norma europea de que el titular del tratamiento proceda a realizar «consultas previas» cuando la evaluación de impacto muestre que la probabilidad de daños para los derechos y libertades de las personas es alto en la operación a realizar. Es decir, una vez constatado el alto nivel de riesgo de la operación, se obliga al responsable del tratamiento a comunicar con la Autoridad de control para verificar si las medidas propuestas permiten garantizar y demostrar una actuación competente. En tal caso, la Autoridad de control podrá exigir la presentación de cualquier documentación adicional a la prevista en el art. 36, así como realizar investigaciones por cuenta propia en virtud de los poderes que le otorga el art. 58 RGPD. En realidad, en dicho supuesto, nos encontramos con un proceso de otorgamiento condicional de autorización para el tratamiento; pues dependerá de la estimación que formule la Autoridad de control la efectiva realización de la operación de tratamiento y su alcance. Constituyendo, al mismo tiempo, una vía eficaz de descargo de responsabilidad por parte del titular del tratamiento que se encuentra *ex ante* con una oportunidad inmejorable de demostrar que ha desarrollado una actividad proactiva orientada hacia la seguridad de los datos manejados sin que, además, la operación se pueda llevar adelante sin el visto bueno y bajo las condiciones específicas que pueda especificar la autoridad independiente de control. Todo ello teniendo en cuenta que el vigente art. 83 RGPD, referido a la imposición de sanciones, toma buena nota del grado de implicación del titular del tratamiento a la hora de graduar la cuantía de las mismas. No en vano, se tiene en cuenta la naturaleza, alcance o propósito de la operación, el número de afectados y el nivel de daños y perjuicios; el grado de intencionalidad o negligencia; las medidas técnicas y organizativas tomadas en aplicación de los principios de responsabilidad proactiva, y de seguridad desde el diseño y por defecto; o la adhesión a códigos de conducta o a mecanismos de certificación que abordo en el siguiente apartado (art. 83.2 RGPD)[11].

[11] En concreto, por ejemplo, en relación con la circunstancia de la adopción o no por el responsable o el encargado del tratamiento de medidas técnicas y organizativas adecuadas, pueden citarse las Sentencias de la Sala 3ª del Tribunal Supremo. 1477/20202, de 10 de noviembre (Ar. 4592); 1620/2020, de 26 de noviembre (Ar. 5044); así como de la Audiencia Nacional de 30 de abril y 14 de mayo de 2021 (Ar. 175714 y 191856), que resuelven, en la mayoría de los supuestos, problemas de posible aplicación retroactiva del RGPD,

Por último, no quiero concluir el presente epígrafe sin destacar que la Agencia Española de Protección de Datos (AEPD) ha aprobado Guías de aplicación del RGPD dirigidas a los responsables del tratamiento con lo que, en uso de las funciones que le otorgan los arts. 57 RGPD y 47 LOPDDG, pretende facilitar la aplicación del Reglamento, la gestión del riesgo y la ya citada evaluación de impacto. En las mismas, se abordan de manera sistemática las principales cuestiones que las corporaciones deben de tener en cuenta, dando orientaciones y recomendaciones que finalmente se concretan en una serie de medidas que puedan ser adoptadas por los titulares del tratamiento. De modo específico, interesa resaltar como distingue, junto con una aproximación sencilla que evalúa de modo acumulativo los diversos factores concurrentes, una aproximación mediante «análisis de dependencias» en la idea de que la presencia de un factor influye de modo directo en el resto, así como en otros tratamientos en curso[12].

IV. EL NECESARIO CRECIMIENTO DE LA CALIDAD DE LA CULTURA CORPORATIVA

La plena vigencia del principio de responsabilidad proactiva comporta, de modo implícito, la necesaria creación y puesta en funcionamiento de una «cultura corporativa de la excelencia en materia de gestión de datos», de modo que los derechos y libertades de los particulares que son objeto de tratamiento por la persona jurídica no se vean comprometidos. La necesidad de demostrar que se han adoptado en cada momento las medidas técnicas y organizativas adecuadas obliga a comprometer con carácter permanente a todo el personal contratado que, en mayor o menor medida, se conecta en su labor diaria con el tratamiento de datos. Es más, los principios de protección de datos desde el diseño y por defecto del art. 25 RGPD coadyuban a su necesaria implementación pues expresamente se habla de medidas organizativas en el momento mismo de decidir los medios a emplear, es decir, desde el principio mismo de la puesta en marcha del sistema de protección de datos[13].

Así, como ocurre con «la cultura del cumplimiento» en relación con la exención de responsabilidad penal de las personas jurídicas del art. 31 bis CP, se hace necesario que desde el nivel directivo se ponga de manifiesto la

[12] Vid. Agencia Española de Protección de Datos*, Guía de gestión del riesgo y evaluación de impacto en tratamientos personales*, edita AEPD, 29 de junio de 2021, pp. 102 y 103.

[13] Agencia Española de Protección de Datos, *Guía de gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, AEPD, junio 2021, pp. 105 a 111, proporciona un amplio repertorio de medidas de gobernanza y políticas de protección de datos que pueden aplicar las empresas.

exigencia en el cumplimiento de unas prácticas que proporcionen un nivel de funcionamiento seguro. Lo anterior porque, evidentemente, son los directivos los que asumen la responsabilidad de la toma de decisiones que implica al conjunto de empleados; pero, al mismo tiempo, también porque resulta aconsejable que participen de una manera protagonista, esto es, dando ejemplo, en la aplicación del conjunto de medidas que garanticen el cumplimiento del RGPD[14].

En última instancia, empero, será el órgano rector de la Sociedad o de la Entidad pública el que, previo informe del responsable de protección de datos asistido por su Delegado (art. 38 RGPD), ponga en marcha el proceso que podrá concretarse en todo un abanico de medidas como pueden ser la publicación de directrices de gestión orientadoras de los comportamientos del personal (sin perjuicio de las externas que adopten la AEPD y el CEPD, Considerando 77); el establecimiento de un protocolo que, a modo de procedimiento, defina la sucesión de pasos a seguir; la publicación periódica de notas informativas o avisos que vayan corrigiendo las desviaciones o disfunciones que se produzcan. Sin olvidar, la necesaria labor de evaluación interna de la calidad de las medidas implementadas que, en caso de existir, debiera recaer en el Delgado de protección de datos que ejerce sus funciones de manera independiente y conectada tanto al nivel ejecutivo del organismo como a la Autoridad de control y a los interesados, completada con auditorías externas si fuera preciso (arts. 38 y 39 RGPD y 36 y 37 LOPDDG). La LOPDDG se ha preocupado de dotar a esta figura de un importante contenido operativo. Por una parte, imponiendo su presencia en un amplio listado de organismos públicos y empresas relevantes que van desde entidades de crédito y aseguradoras hasta centros sanitarios y federaciones deportivas. Y, por otra, exigiendo su necesaria cualificación teórica y práctica, preferentemente universitaria y con conocimientos especializados en derecho que podrá acreditarse mediante mecanismos de certificación (art. 34.1 y 35). Se trata, en cualquier caso, de dejar claro que el organismo mantiene una política de actuación conforme al Reglamento en todo momento; sancionando las actuaciones y actitudes que pongan en riesgo o directamente incumplan el sistema de protección de datos diseñado. Lo que se verá reforzado por el convencimiento de que la aplicación efectiva de la nueva ética corporativa en materia de protección de datos contribuye, por sí misma, a conseguir el éxito de la organización en la medida en que proyecta una imagen de segura y fiable de la entidad.

El establecimiento de una cultura de responsabilidad proactiva en la protección de datos personales se puede ver incentivada, a su vez, mediante la

[14] RIBAS X., Abogado, *¿Qué es la cultura de cumplimiento, cómo se mide y cómo se acredita?*, blog ribas y asociados, 9 de marzo de 2016, www.legaltoday.com.

posible adopción por la entidad de otros instrumentos previstos en el RGPD que ayudan a alcanzar el deseado nivel de eficacia en el funcionamiento del sistema de protección de datos. Me estoy refiriendo en primer lugar a la posible suscripción de un Código de Conducta (art. 40 RGPD y art. 38 LOPDDG) que se haya elaborado por empresas o grupos de empresas del sector en el que desarrolle su actividad, organismos públicos y judiciales, asociaciones u otros organismos representativos responsables y encargados del tratamiento y que se vea validado por la Autoridad de control, por el Comité Europeo de Protección de Datos o la Comisión. Nos encontramos ante un supuesto de autorregulación sancionada por la Instancia independiente de control que va a propiciar el que una actuación acorde con su contenido, atendidos con proporcionalidad los distintos factores concurrentes, se declare conforme con el RGPD (art. 98 RGPD)[15]. De manera que se estará en condiciones de demostrar la exigida probidad en la actuación del titular del tratamiento. Pero, además, su aplicación servirá para establecer un principio de prueba que permita eximir o al menos atenuar la responsabilidad del responsable y del encargado de protección de datos (arts. 24.3, 28.5 y 83.2.j) RGPD), teniendo en cuenta que la vulneración del principio de responsabilidad proactiva se tipifica, por sí mismo, como infracción muy grave (art. 72.1.a) LOPDDG).

Un segundo instrumento de carácter voluntario previsto en la normativa europea que igualmente coadyuva a la implantación de la necesaria cultura de excelencia en la protección de datos se concreta en la obtención de mecanismos de certificación o sellos y marcas de garantía (art. 42 RGPD) que igualmente permite facilitar el cumplimiento de la normativa de protección de datos y servir de prueba de la necesaria probidad del titular y del encargado[16]. Lo que podrá

[15] La Agencia Española de Protección de Datos*, Cumple tus deberes. Medidas de cumplimiento. Códigos de Conducta*, AEPD, 21 de mayo de 2021, www.aepd.ess, define los códigos de conducta como «*una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse por sí mismas a partir de la normativa establecida*». No obstante, ha de tenerse en cuenta que, en el ámbito de la protección de datos personales, los códigos de conducta han de ser finalmente validados por la Comisión Europea, el CPDE, o las Autoridades del control por lo que encajan, más específicamente, con la idea de corregulación que adquiere carácter normativo para los sujetos adheridos voluntariamente a su contenido, con miras a la consecución de fines de interés general. Un *tertius genus* entre reglamento y orientación, entre *hardlaw* y *softlaw*. ESTEVE PARDO J., *Autorregulación. Génesis y Efectos*, Aranzadi, 2002, p. 39, pone el acento en la conveniencia del encuadramiento del código de conducta en una previa normativa pública que lo incentive y oriente; alcanzándose así un adecuado equilibrio entre fines públicos y privados.

[16] Agencia Española de Protección de Datos, Agencia de Protección de Datos de Cataluña y Agencia Vasca de Protección de Datos, *Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento*, edición conjunta de AEPD, APDCAT y AVPD, 2016, p. 14, resalta que los responsables del tratamiento, encargados y subencargados tiene la posibilidad de adherirse a códigos de conducta, mecanismos de certificación, marcas y sellos de calidad dentro

completarse con la información que proporcione el obligado registro de actividades (art. 30 y Considerando 82 RGPD), como elemento probatorio de naturaleza imperativa que permite, en última instancia, resolver la dudas que se plantean sobre la conformidad a la norma del tratamiento que se evalúa.

V. CONCLUSIONES

El principio de responsabilidad proactiva constituye, en el marco del nuevo RGPD, el concepto medular de la nueva regulación en cuanto comporta un cambio de paradigma en la legislación de protección de datos personales. Se pasa de una regulación jurídica orientada al cumplimiento de sus preceptos a una normativa que promueve la diligencia debida del responsable del tratamiento en cada una de las actuaciones que realiza.

La responsabilidad proactiva, de otra parte, se configura como un concepto abierto pendiente de concreción en cada supuesto específico mediante la evaluación de la actuación realizada a la luz de los factores concurrentes y de las medidas organizativas y técnicas adoptadas por el titular del tratamiento. Se asimila, por consiguiente, a la noción de concepto jurídico indeterminado por cuanto la aptitud para demostrar la probidad en el diseño y la gestión del tratamiento se verán concretadas mediante un juicio a hoc de la Autoridad independiente de control o del Órgano judicial.

Nos encontramos, de otra parte, ante un concepto evolutivo por cuanto el progreso social y el desarrollo de la técnica plantean nuevos retos y niveles de cumplimiento. A lo que han de añadirse las prescripciones y orientaciones que vayan aportando diferentes fuentes de conocimiento y cumplimiento del Derecho. Me refiero, lógicamente, a las reglas interpretativas deducidas de la jurisprudencia, de las que ya contamos con los primeros ejemplos en relación con el aludido principio por parte del TJUE. E igualmente con la paulatina aprobación y entrada en vigor de Códigos de conducta y Directrices provenientes del CEPD y de las Autoridades de control.

También es de destacar, por último, la eficacia esencialmente horizontal del principio de rendición de cuentas que condiciona de manera decisiva la aplicación de toda la normativa de protección de datos. Comenzando por la regulación relativa a la gestión del riesgo que gira en torno a la necesidad de que disminuir los riesgos inherentes al tratamiento; pero salvaguardando siempre que el responsable del tratamiento sea capaz de demostrar la adecuación de su

de los esquemas previstos en el RGPD (art. 24.3 y 27.5 RGPD) como medio para acreditar el cumplimiento de sus obligaciones.

intervención. Asimismo, destaca el desarrollo de una serie de instrumentos que contribuyen a acreditar una política coherente de protección de datos, como los ya aludidos códigos de conducta, la obtención de mecanismos de certificación o de marcas o sellos de garantía; sin olvidar las especiales cautelas que, a partir de ahora, se mantienen en el examen de los documentos (decisiones de conformidad, cláusulas de garantías, normas corporativas vinculantes) que permiten la transferencia internacional de datos a terceros Estados. De manera que se consiga una efectiva consecución de los objetivos del RGPD, la protección de los derechos y libertades de las personas en un ámbito de continua circulación de datos personales.