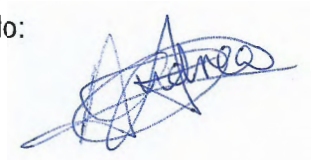
UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Facultad de Economía, Empresa y Turismo

DOBLE GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS Y DERECHO

El Reglamento General de Protección de Datos y su impacto en las organizaciones: la figura del Delegado de Protección de Datos

Presentado por: Andrea Guillén Gil
45331924 M

Fdo: 

Las Palmas de Gran Canaria, a 3 de febrero de 2017

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

AEPD Agencia Española de Protección de Datos

BDSG *Bundesdatenschutzgesetz* (Ley Federal de Protección de Datos)

CDFUE Carta de Derechos Fundamentales de la Unión Europea

DPIA *Data Protection Impact Assessment* (Evaluación de impacto relativa a la protección de datos)

DPO *Data Protection Officer* (Delegado de Protección de Datos)

LOPD Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal

RGPD Reglamento General de Protección de Datos

SEPD Supervisor Europeo de Protección de Datos

TFUE Tratado de Funcionamiento de la Unión Europea

WP29 *Article 29 Working Party* (Grupo de Trabajo del Artículo 29)

I. INTRODUCCIÓN

Según la Agencia Española de Protección de Datos (en adelante, AEPD), el derecho fundamental a la protección de los datos personales reconoce la facultad del individuo de controlar sus datos de carácter personal así como la capacidad para disponer y decidir sobre los mismos (Agencia Española de Protección de Datos, 2004).

En la Sociedad de la Información en la que actualmente vivimos, se lleva a cabo diariamente el tratamiento de una cantidad astronómica de datos personales los cuales debemos facilitar para hacer uso de diferentes servicios cotidianos. Estos datos constituyen información valiosa que permite identificar a una persona directa o indirectamente. En este sentido ya no sólo nos estamos refiriendo a los datos obvios relativos al nombre, apellidos o número de DNI, sino también a un abanico de datos mucho más amplio que abarca desde el número de matrícula del coche o de la tarjeta bancaria hasta las huellas dactilares o los datos biométricos. Esto sin mencionar la información que cada uno expone libremente de su vida privada en las redes sociales. No es de extrañar que desde hace ya unos años se haga referencia a los datos como el petróleo de nuestra sociedad (Palmer, 2006), y es que estos revelan quienes somos y todo lo referente a nuestra situación económica y familiar, salud, relaciones, opiniones políticas y religiosas, aficiones e intereses, capacidades y habilidades, y un largo etcétera.

En este sentido juega un papel muy importante el *Big Data*, que se trata de una herramienta caracterizada por un veloz y elevado volumen de datos que no se ajusta a una estructura definida (Dumbill, 2012) y cuya información es recabada por corporaciones y gobiernos y analizada por algoritmos. El valor del *Big Data* radica en la agregación de datos personales junto con otras herramientas como la minería de datos, la elaboración de perfiles o identificación de *outliers*, de forma que los patrones y correlaciones sean detectados, relevantes y factibles. *Big Data* se puede usar para identificar tendencias generales pero también puede ser tratada para afectar directamente a individuos (González Fuster & Scherrer, 2015), permitiendo la elaboración de perfiles para realizar publicidad personalizada, la determinación de la concesión de un crédito, el ofrecimiento de un seguro más o menos caro o el seguimiento de delincuentes.

Siendo indiscutible el progreso y el aumento de la calidad de vida que nos proporciona la tecnología, es absolutamente necesario establecer una ponderación entre el derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación y el uso de las

nuevas tecnologías. Además del derecho de los ciudadanos a saber quién gestiona nuestros datos y con qué fines.

Por ello, el legislador consagra este derecho como derecho fundamental en la Carta de Derechos Fundamentales de la Unión Europea (en adelante, CDFUE) en su artículo 8.1: "*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*". A su vez, el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) se refiere a este derecho en los mismos términos que establece el artículo 8.1 CDFUE.

Como podemos observar, ambos textos recogen el derecho fundamental a la protección de los datos de carácter personal como un derecho independiente.

En la actualidad, este derecho está desarrollado en el ámbito europeo por la Directiva 95/46/CE[1].

A nivel nacional, la Constitución Española de 1978 indica en su artículo 10: "*La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento de orden político y de la paz social*.", y el artículo 18.4 establece lo siguiente: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*." Cabe destacar que el desarrollo normativo de este artículo está contenido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

De ambos artículos de la Constitución deriva, en el ámbito estatal, el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre.

Como se ha mencionado anteriormente, el actual régimen jurídico de la protección de datos en Europa, sentado sobre las bases de la CDFUE y del TFUE, viene marcado por las pautas establecidas en la Directiva 95/46/EC. Dicha Directiva, como tal, no gozó de aplicación directa y tuvo que ser transpuesta por las normas nacionales de cada Estado Miembro. En el caso de España, esta ley de transposición es la ya referida LOPD.

[1]Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DO L 281 de 23.11.1995, p. 31-50).

Esto ha derivado en un conglomerado de leyes nacionales semejantes pero no idénticas, donde cada Estado Miembro ha interpretado de diverso modo la Directiva. Aún siendo estas leyes similares, las autoridades nacionales de protección de datos las han interpretado y aplicado de diferente manera. Como resultado, las organizaciones que tenían sus negocios en diferentes países de la Unión Europea han tenido que cumplir con diferentes principios, obligaciones o multas en función del país.

Desde la entrada en vigor de la Directiva, han surgido cambios significativos en el uso de la información, tanto en el mundo empresarial como en el contexto personal. Muchas herramientas y dispositivos que actualmente son de uso común, como los *smartphones* o los *wearables,* no existían en aquel entonces. La rápida transformación tecnológica ha cambiado nuestra economía y vida social, y ha facilitado, y lo seguirá haciendo, aún más la libre circulación de datos personales tanto dentro como fuera de la Unión. En este sentido, se trata de una Directiva obsoleta y sobrepasada por la vertiginosa revolución tecnológica (López Aguilar, 2013).

Por ello, la Directiva ya no es útil como respuesta para hacer frente al mundo interconectado en el que vivimos, y para la cual no fue diseñada. Ante revoluciones tecnológicas como el *Big Data*, *Open data*, el Internet de las Cosas o la Inteligencia Artificial, la sociedad necesita de una nueva regulación que sea aplicable a estos nuevos acontecimientos. Estos avances han marcado el ritmo y la necesidad de crear un marco más sólido y coherente para la protección de datos en la Unión Europea, pues a pesar de que los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada.

Precisamente para superar estas dificultades se ha publicado en mayo de 2016 el Reglamento (UE) 2016/679[2] (Reglamento general de protección de datos, en adelante, RGPD), el cual pretende reforzar y armonizar la protección de datos en la Unión Europea y que será aplicable en mayo de 2018.

El objetivo del presente trabajo es comprender las novedades fundamentales establecidas por dicho Reglamento e indicar el impacto que producirá su aplicación en las administraciones

[2] Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (DO L 119 de 04.05.2016, p. 1-88).

públicas y en las empresas privadas. Para ello, en primer lugar, se muestra el marco teórico, donde se presenta el proceso que ha transcurrido hasta la publicación del RGPD. Los aspectos metodológicos recogen el contenido esencial que se va a tratar, la estructura del trabajo y el objetivo del mismo. A continuación se tratan las novedades más relevantes establecidas por el Reglamento relacionadas con los principios rectores, los derechos de los ciudadanos y las obligaciones para las organizaciones. Por último, en el epígrafe referente a la especial referencia a la figura del Delegado de Protección de Datos, se presenta esta nueva figura que será obligatoria para las empresas públicas y privadas bajo determinadas circunstancias. Con este fin, se señalarán diferentes aspectos relacionados con su definición, designación, posición, funciones y responsabilidad. En las conclusiones, se destaca la importancia de que las empresas del sector público y privado centren sus esfuerzos en adaptarse a esta nueva norma.

Se pretende, pues, analizar dichas novedades para comprender los desafíos que las organizaciones afrontarán en 2018. Donde no sólo se deberá cumplir con una nueva norma, sino adaptarse a un cambio estructural que abarca todos los ámbitos de la organización. El más significativo de ellos es un cambio de filosofía, ya que el espíritu del legislador europeo en este Reglamento es establecer un cambio de paradigma orientado a promover y fomentar la cultura de la protección de datos a todos los niveles jerárquicos.

Todos estos cambios sustanciales en lo relativo al derecho fundamental a la protección de datos personales supone para las empresas públicas y privadas la implementación de mecanismos y medidas necesarias que requerirá de concienciación, planificación e inversión y tiempo. Por lo que, aunque mayo de 2018 aún parezca lejano, las organizaciones deben comenzar ya a adaptarse al Reglamento para evitar que su imagen quede dañada, además de recibir multas millonarias.

II. MARCO TEÓRICO

Este Reglamento es el resultado de un largo proceso de varios años de negociaciones entre el Parlamento Europeo, la Comisión Europea y el Consejo (Ver Anexo I). El origen que dio lugar a estas negociaciones fue la conferencia "*Personal data – more use, more protection*?" organizada por la Comisión Europea el 19 y 20 mayo de 2009, la cual formaba parte de las consultas públicas de la Comisión sobre el posible desarrollo del derecho fundamental a la protección de los datos.

Ante esta invitación a consultas, el 1 diciembre de 2009, el Grupo de Trabajo del Artículo 29[3] (*Article 29 Working Party,* en adelante*, WP29*) y el Grupo de Trabajo sobre Policía y Justicia (*Working Party on Police and Justice, WPPJ*) publicaron un documento llamado «*Future of Privacy*»[4], donde se recalcaba la necesidad de establecer un nuevo marco legal. Ya el 4 de noviembre de 2010, la Comisión Europea[5] planteó la necesidad de una aplicación homogénea en la Unión Europea del derecho a la protección de los datos personales.

Tras la consulta a diversos actores implicados, así como los múltiples dictámenes emitidos por el Grupo de Trabajo del Artículo 29 y el Supervisor Europeo de Protección de Datos (en adelante, SEPD), tanto el Consejo[6] como el Parlamento Europeo[7] mostraron en 2011 su apoyo a la reforma del marco de la protección de datos.

Es en 2012 cuando comienza el periodo de arduas negociaciones con la Propuesta de Reglamento[8] publicada por la Comisión Europea el 25 de enero de 2012. Tras numerosos debates, reuniones, votaciones, relevantes modificaciones, dictámenes del Comité Económico y Social Europeo[9] y del Comité de las Regiones[10], así como del WP29 y del SEPD, en diciembre de 2015 los negociadores del Parlamento y del Consejo, que tenían posturas diferenciadas sobre aspectos relevantes en años anteriores, llegaron a una versión común del Reglamento. En los días posteriores, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) aprobó el texto acordado y el Comité de Representantes Permanentes (COREPER) lo confirmó y lo presentó para su adopción por el Consejo y posteriormente por el Parlamento, ya con la intención de que el Reglamento entrase en vigor en la primavera de 2018. Finalmente, el RGPD se publicó el 4 de mayo de 2016 en el Diario Oficial de la Unión Europea.

[3] El Grupo de Trabajo del Artículo 29 está contemplado en el propio artículo 29 de la Directiva 95/46/CE. Tiene carácter consultivo e independiente y está compuesto por un representante de las autoridades de protección de datos de cada Estado Miembro, representantes del Supervisor Europeo de Protección de Datos y representantes de la Comisión Europea.

[4] «*Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.*» (02356/09/EN, WP 168)

[5] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: «Un enfoque global de la protección de los datos personal es en la Unión Europea», COM(2010) 609 final.

[6] «*Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protectionin the European Union*.» (5980/3/11, REV 3)

[7] Resolución del Parlamento Europeo, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI))

[8] COM(2012) 11 final

[9] DO C 229 de 31.7.2012, p.90

[10] DO C 391 de 18.12.2012, p.127

III. ASPECTOS METODOLÓGICOS

El propósito de este trabajo es abordar las principales novedades que el Reglamento aporta en materia de protección de datos, las cuales se centran en tres aspectos fundamentales: nuevos principios, nuevos derechos de los ciudadanos y nuevas obligaciones para empresas, administraciones y otras entidades.

Para ello, en cada apartado se expondrá, en primer lugar, el contenido recogido en el Reglamento, sus especificidades y características, así como aquellos elementos en los que se entiende que se hace necesaria una aclaración puesto que no quedan delimitados, y los aspectos que debieron incluirse. A su vez, se señalarán las consecuencias más significativas de la norma para las empresas públicas y privadas y se propondrán, en su caso, medidas prácticas que las organizaciones deberán llevar a cabo para el cumplimiento de la misma.

Esta información será recabada de diversas fuentes y en diversos idiomas. La fuente principal será el RGPD en sus versiones en español, inglés y alemán, consultas y artículos de expertos, libros, conferencias, vídeos y webs, así como los conocimientos adquiridos durante las prácticas curriculares en el Supervisor Europeo de Protección de Datos y la entrevista realizada al Europarlamentario Juan Fernando López Aguilar recogida en el Anexo I.

IV. NOVEDADES INTRODUCIDAS POR EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. Cuestiones generales

Es necesario advertir que tal y como recoge el considerando 9 del Reglamento, "*los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos*", por lo que este RGPD no supone un cambio radical en relación con la Directiva 95/46/CE, pero sí una evolución sustancial en aras de conseguir una respuesta eficaz al entorno tecnológico actual y futuro.

En este sentido, hay que señalar en primer lugar que el hecho de que se haya optado por un Reglamento ya implica toda una declaración de intenciones, debido a su carácter directamente vinculante para los Estados miembros e invocable por los ciudadanos ante los Tribunales, y es que su finalidad es garantizar una aplicación coherente y homogénea de protección de datos en todos los países de la Unión Europea y la libre circulación de datos.

Tal y como recoge el considerando 9, el hecho de que el instrumento jurídico fuese una Directiva, con su necesario desarrollo por una ley nacional, ha ocasionado que la protección de datos se haya aplicado de "*manera fragmentada*" ya que cada Estado ha ejecutado la Directiva de distinta manera y ha dotado de diferentes niveles de protección a los datos personales. Esta situación ha dificultado la libre circulación de los datos personales y ha supuesto un "*obstáculo al ejercicio de las actividades económicas a nivel de la Unión*".

Sin embargo, cabe decir que aunque el Reglamento sea de aplicación directa, el mismo establece en el considerando 8 que en ciertos supuestos las normas sean "*especificadas o restringidas*" por las leyes nacionales. Es decir, seguirá siendo necesaria una ley estatal que determine ciertos aspectos del Reglamento. En el caso de España, se está redactando una nueva Ley Orgánica de Protección de Datos, que se adapte a los avances tecnológicos y a la globalización y, por supuesto, al Reglamento.

Las cuestiones más relevantes están fijadas en el Reglamento, y a raíz de éste, los Estados Miembros tienen cierto margen de maniobra para especificar en mayor grado la aplicación de las normas atendiendo, entre otros, a criterios sociales o culturales, como por ejemplo el consentimiento de menores de edad.

El hecho de que el Reglamento supone una evolución, y no una sustitución, lo observamos atendiendo al articulado del mismo y al propio contenido. Mientras que la Directiva contiene 34 artículos, 72 considerandos y 8 definiciones; el Reglamento cuenta con 99 artículos, 173 considerandos y 26 definiciones. Estableciendo así más ejemplos y nociones, mayor claridad a los conceptos, mayor capacidad de interpretación y, en definitiva, adaptabilidad a un entorno, definido por el cambio (Maeztu, 2016).

Como ejemplo de ello, cabe resaltar aquí por su gran importancia la evolución de la definición de «datos personales», cuya noción es básica para saber cuándo estamos ante un dato de carácter personal y, por lo tanto, cuándo es de aplicación este Reglamento.

La Directiva 95/46/CE lo define de la siguiente manera en su artículo 2 a): "*toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*."

El Reglamento en su artículo 4.1 lo define como: "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador,* ***como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea*** *o uno o varios elementos propios de la identidad física, fisiológica,* ***genética****, psíquica, económica, cultural o social* ***de dicha persona***".

Como se puede observar, aunque la definición es muy similar, el legislador incorpora ejemplos, los cuales son muy amplios para permitir que un número mayor de tipos de datos sean considerados personales, ya que con los avances de la tecnología la delimitación de estos ejemplos supondría que futuras tipologías de datos no queden regulados y amplía el hecho de que los datos genéticos también sean considerados datos personales. En definitiva, se pretende, siguiendo las líneas establecidas en la Directiva, poder abarcar el máximo número de situaciones que se puedan dar en un futuro, para evitar una pronta obsolescencia de la norma.

1.1 Entrada en vigor, aplicación y desarrollo

Tal y como recoge el artículo 99 RGPD (Ver Anexo II), el Reglamento entró en vigor el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018. Durante estos dos años, las normas nacionales que desarrollan la Directiva 95/46/EC, en el caso de España la LOPD, como la propia Directiva seguirán siendo de aplicación.

En este tiempo, como se ha mencionado anteriormente, los Estados miembros deben elaborar normas que especifiquen en mayor grado la aplicación de ciertas normas recogidas en el Reglamento. En este sentido, España está ya trabajando en un borrador para una nueva LOPD. Dichas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni excederse de los poderes para los que están facultados por el Reglamento.

A medida que se profundiza en el estudio del RGPD se observa la cantidad de implicaciones que contiene para las organizaciones. Por ello, durante este periodo de transición, las empresas y organismos públicos deben comenzar a planificar la aplicación de este Reglamento desde el punto de vista tecnológico, financiero y de recursos humanos, porque las consecuencias del incumplimiento acarrearán importantes sanciones económicas como daños en la imagen de marca difícilmente reparables, en el caso de empresas privadas.

1.2 Ámbito de aplicación

En cuanto al ámbito de aplicación material, el artículo 2 RGPD establece que: "*El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales**,** así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.*" En este sentido, cabe puntualizar que según el artículo 4, se entenderá por «tratamiento», "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*"

El RGPD no será de aplicación a las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión; a las actividades de los Estados miembros comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; al tratamiento de datos efectuado por una persona física en el ejercicio de actividades personales o domésticas ni a las actividades objeto de la Directiva 2016/680**.**

El artículo 3 del Reglamento recoge la novedad que indiscutiblemente supone un gran impacto a nivel mundial: el ámbito de aplicación territorial. Se establece que el Reglamento se aplicará "*al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente** de que el tratamiento tenga lugar en la Unión o no*", así como "*al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado **no establecido en la Unión***" para el caso de que realicen tratamientos derivados de la oferta de bienes o servicios o como consecuencia de una monitorización y seguimiento del comportamiento de personas en la Unión.

Por lo tanto, el Reglamento se aplicará a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, y se amplía a responsables y encargados no establecidos en la UE en los supuestos mencionados anteriormente. Estas organizaciones deberán nombrar un representante en la Unión Europea según el artículo 27, que actuará como punto de contacto de las autoridades de supervisión y de los ciudadanos.

Este nuevo panorama dotará de una garantía adicional a los ciudadanos residentes en la Unión Europea, ya que el Reglamento será aplicable a empresas que, hasta ahora, tratan datos de sujetos residentes en la Unión y, sin embargo, se rigen por normativas que, en la inmensa mayoría de supuestos, no ofrecen el mismo nivel de protección.

1.3 Sujetos

De los sujetos establecidos en el RGPD, podemos destacar aquellos que se encuentran en el seno de las organizaciones, así como al interesado, y la autoridad de control.

Los sujetos mencionados en el RGPD que desarrollan su labor para las empresas u organismos públicos son los referidos en la siguiente tabla. En ella, se señala la definición que el propio Reglamento establece para ellos en el artículo 4 RGPD, así como la responsabilidad que tienen ante incumplimientos de dicha norma.

Tabla 1. Sujetos relacionados con el tratamiento de los datos personales

	DEFINICIÓN	**RESPONSABILIDAD POR INCUMPLIMIENTO DEL RGPD**
Delegado de Protección de Datos (DPO)	El RGPD no establece una definición del DPO. (Ver Epígrafe. V. ESPECIAL REFERENCIA A LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS)	No tiene responsabilidad
Responsable del tratamiento	"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**"	Responsabilidad total (Artículo 24.1 RGPD)
Encargado del tratamiento	"la persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable del tratamiento**"	Responsabilidad limitada (Artículos 28 y 29 RGPD)

Fuente: elaboración propia

Es muy importante distinguir estos sujetos ya que son los principales obligados por el RGPD, y su labor es crucial para el cumplimiento del Reglamento.

Por otro lado, es necesario mencionar al «interesado», que aunque su definición no conste en el RGPD, es aquella persona titular de los datos personales en cuestión. De ahí que de modo más acertado, se denomine en inglés *data subject*. Sin embargo, la denominación de *betroffene Person* en alemán, como en la versión española, significa persona interesada o afectada.

Con respecto a la «autoridad de control», el artículo 51.1 prevé: "*Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión*." En el caso de España, la autoridad de control es la ya referida Agencia Española de Protección de Datos (AEPD).

2. Principios

2.1 Responsabilidad proactiva o *accountability*

Recogido en el artículo 5.2 RGPD, supone que los responsables del tratamiento, además de cumplir con las exigencias de la norma, deben ser capaces de demostrar que llevaron a cabo todas las medidas necesarias para cumplir con las obligaciones establecidas, debiendo asumir una total responsabilidad por sus acciones u omisiones. Esta obligación se hace extensible a los encargados del tratamiento según los artículos 28 y 29 RGPD.

Para dar cumplimiento a este principio, el Reglamento recoge en el Capítulo IV diferentes mecanismos preventivos y actuaciones que deben ser implementadas por las personas implicadas en el tratamiento de datos personales que aseguren y demuestren el cumplimiento. Algunas de estas medidas son:

- El cumplimiento de los principios de protección de datos desde el diseño y por defecto (Artículo 25)
- La llevanza de registros de todos los tratamientos (Artículo 30)
- La implementación de mecanismos que garanticen un alto nivel de seguridad de tratamiento (Artículo 32)
- Las obligaciones de notificación y comunicación de las violaciones de seguridad (Artículos 33 y 34)
- La evaluación de impacto relativa a la protección de datos (Artículo 35)
- La autorización y consulta previa a la autoridad de control (Artículo 36)
- La designación de un Delegado de Protección de Datos (Artículo 37)
- La adhesión a códigos de conducta (Artículo 40) y a certificaciones y sellos de calidad (Artículo 42)

La responsabilidad proactiva implica numerosos retos para las organizaciones, especialmente en lo referente a la implementación de medidas técnicas y organizativas que aseguren y demuestren el cumplimiento. Pero además de las herramientas que establece el legislador europeo, existen fundamentalmente otros dos aspectos que deben ser conjuntamente llevados a cabo por las organizaciones para que la aplicación de las medidas anteriormente mencionadas sea eficaz.

En este sentido, se deben establecer reglas internas sobre protección de datos que estén aprobadas y apoyadas por el más alto nivel jerárquico de la organización. Y, a su vez, es absolutamente primordial sensibilizar a los trabajadores de todos los niveles de la organización de la importancia de la protección de datos. Para ello se deberá formar a la plantilla sobre los derechos fundamentales que están siendo expuestos mediante los tratamientos de datos, la implementación de las medidas preventivas y las consecuencias que acarrean tratamientos inadecuados. La educación y la concienciación son elementos básicos que se deben reforzar en el seno de las organizaciones, ya que en muchas ocasiones no falla la tecnología sino el ser humano, debido a su poca diligencia, negligencia o de forma intencionada.

Por todo esto, se puede aseverar que este principio, al ir más allá del cumplimiento de las normas, supone un cambio en la cultura empresarial (Supervisor Europeo de Protección de Datos, 2016).

2.2 Consentimiento

El RGPD define el consentimiento en el artículo 4 en los siguientes términos: "*toda manifestación de voluntad libre, específica, informada e* ***inequívoca*** *por la que el interesado acepta, ya sea* ***mediante una declaración o una clara acción afirmativa****, el tratamiento de datos personales que le conciernen*", completando así la definición establecida en la Directiva 96/45/CE: "*toda manifestación de voluntad, libre, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernan*".

Volviendo al Reglamento, el considerando 32 clarifica que una "acción afirmativa" puede incluir "*marcar una casilla de un sitio web", "escoger parámetros técnicos para la utilización de servicios de la sociedad de la información"* o *"cualquier otra declaración o conducta"*. Además, recalca que "*el silencio, las casillas ya marcadas o la inacción*" no deben implicar que se está dando consentimiento.

Además, el RGDP incluye otros aspectos adicionales relativos al consentimiento. En primer lugar, el artículo 7.3 establece el derecho de retirada de consentimiento, el cual podrá ser ejercido en cualquier momento. Una vez retirado, el interesado tiene el derecho a que sus datos sean borrados y dejen de ser tratados. En segundo término, el considerando 43 añade que se presume que el consentimiento no se ha prestado libremente cuando "*exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública*". Por último, el RGPD añade que el consentimiento debe ser prestado para cada tratamiento, debiéndose distinguir de "*los demás asuntos*" (Artículo 7).

A su vez, hay determinadas circunstancias para las que se requiere un consentimiento **explícito**. Según el artículo 9 el consentimiento deberá ser explícito cuando se trata de categorías especiales de datos personales. Para el caso de que el interesado sea objeto de "*una decisión basada en el tratamiento automatizado, incluida la elaboración de perfiles*" (Artículo 22) y cuando el interesado autorice la transferencia de sus datos personales a otros países que no cuentan con unas garantías de protección adecuado (Artículo 49).

En lo relativo a menores, el artículo 8 RGPR introduce una protección específica limitando su capacidad de prestar consentimiento sin una autorización. Siempre que el menor tenga menos de 13 años será necesaria una autorización en todos los casos y entre los 13 y los 16 será cada Estado el que decida la edad hasta la que será necesaria la autorización. En este sentido, el responsable "*hará esfuerzos razonables*" para comprobar que el consentimiento fue autorizado por el titular de la patria potestad o tutela.

2.3 Transparencia

El Reglamento le da tal importancia a la transparencia que lo regula como principio (Artículo 5) y como derecho (Sección 1 del Capítulo III), teniendo en cuenta que su contenido no varía, y para evitar su redundancia, la trataremos únicamente en este apartado como principio. En su configuración como tal, está mencionado en el artículo 5.1, aunque son los considerandos 39 y 58 los que precisan su significado.

El considerando 39 establece que, "*El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro*." Y continúa añadiendo, "*En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y*

deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados."

En este sentido, el considerando 58 especifica la necesidad de cumplir con el principio de transparencia, especialmente "*en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen*". Además, este considerando prevé la posibilidad de utilizar iconos normalizados para que sea más sencillo entender la información que se nos está prestando y refuerza el otorgamiento de una protección específica a los niños.

Teniendo estos preceptos en cuenta, el Reglamento lo que pretende es que los avisos legales y políticas de privacidad sean simples y fácilmente entendibles para cualquier ciudadano.

La realidad es que la gran parte de la sociedad no lee, por ejemplo, los términos y condiciones de uso de las redes sociales, directamente las acepta. Y es que no nos importa el contenido de ese documento porque no somos conscientes de las consecuencias. Para ello, se ilustra con un ejemplo el contenido de las condiciones de uso y política de privacidad de Facebook ya que es la red social más popular, con 1,65 billones de usuarios activos al mes. Pues bien, la aceptación de la política de privacidad tiene, entre otras, las siguientes consecuencias (Burgueño, 2015):

- Facebook puede analizar y tratar la libreta contactos, accediendo así a los datos de estas personas.
- Cuando se accede a Facebook, éste puede conocer los siguientes datos del dispositivo: sistema operativo, nombres y tipos de archivos, ubicación del dispositivo, información sobre la conexión (operador de telefonía, tipo de navegador, zona horaria, número de teléfono o dirección IP)
- Se le concede una licencia no exclusiva, transferible, con derechos de sublicencia, libre de regalías y aplicable en todo el mundo para utilizar cualquier contenido de propiedad intelectual que se publique en Facebook o en conexión con Facebook.

Por si no fuera suficiente, esos datos los puede compartir con otros usuarios de la red social, servicios de terceros, empresas del grupo Facebook o servicios de analítica. Es decir, nuestros datos se venden. Esas empresas que los compran, llamadas *data brokers*, son los que, haciendo uso de Big Data, pueden conocer nuestra situación económica y familiar, la

ubicación de nuestra casa, trabajo, lugar de veraneo o comida favorita. En definitiva, pueden saber más de nosotros que nosotros mismos.

Cualquier aplicación o red social gratuita la pagamos con nuestra privacidad (Alonso, 2016), y debe ser cada individuo quien considere si es justo pagar ese precio. Por ello, la información contenida en estos documentos donde damos nuestro consentimiento debe ser clara, concisa e inteligible para cualquier persona, y que así cada cual pueda tomar una decisión bien informada.

3. Derechos del interesado

El RGPD dedica el Capítulo III a los derechos del interesado. De todos los derechos referidos, en las próximas páginas nos detendremos en aquellos que contengan novedades significativas y los nuevos derechos configurados. Los derechos del interesado son los siguientes:

- Transparencia (Artículo 12, Considerandos 58 a 60)
- Información (Artículos 13 y 14, Considerandos 60 a 62)
- Derecho de acceso (Artículo 15, Considerandos 63 y 64)
- Derecho de rectificación (Artículo 16, Considerando 65)
- Derecho de supresión o derecho al olvido (Artículo 17, Considerandos 65 y 66)
- Derecho a la limitación del tratamiento (Artículo 18, Considerando 67)
- Derecho a la portabilidad de los datos (Artículo 20, Considerando 68)
- Derecho de oposición (Artículo 21, Considerandos 69 y 70)
- Decisiones individuales automatizadas, incluida la elaboración de perfiles (Artículo 22, Considerandos 71 y 72)

3.1 Derecho de supresión o derecho al olvido

Antes de adentrarnos en la regulación del derecho al olvido establecido por el RGPD, es necesario subrayar por su grandísima importancia, la sentencia del Tribunal de Justicia de la Unión Europea sobre el caso *Google vs. España*[11]. En ella se establece que los tratamientos de datos llevados a cabo por los motores de búsqueda en Internet están sometidos a las normas de protección de datos de la Unión Europea y, a su vez, reconoce el derecho de las

[11] Sentencia del Tribunal de Justicia de 13 de mayo de 2014, *Google Spain SL.* y *Google Inc.* c. *Agencia Española de protección de datos (AEPD)* y *Mario Costeja González,* C-131/12 [ECLI:EU:C:2014:317]

personas a solicitar que los enlaces a sus datos personales no figuren en los resultados de una búsqueda de internet realizada por su nombre.

Recogiendo lo señalado por el Tribunal, el RGPD establece en su artículo 17.1 lo siguiente respecto al derecho al olvido: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1."

Además, el artículo 17.2 prevé: "*Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos*."

Sin embargo, el artículo 17.3 recoge las limitaciones del derecho al olvido, señalando que los preceptos previamente mencionados no se aplicarán cuando el tratamiento sea necesario para: " *a) para ejercer el derecho a la libertad de expresión e información;*

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones."

En este sentido, es de resaltar la colisión que el propio Reglamento recoge entre el derecho al olvido y el derecho a la libertad de expresión e información. Así, como manifiesta A. Rallo Lombarte (2014, pp. 159-160), "el derecho al olvido en internet tiene en los medios de comunicación online su más conflictivo escenario al ofrecer una aparentemente insalvable colisión entre el derecho a la protección de datos y la manifestación prototípica de la libertad de expresión y el derecho a la información."

En cualquier caso, es de reconocer de forma muy positiva, el reforzamiento del derecho al olvido en estos últimos años, aunque aún quedan avances significativos por llevar a cabo en la materia en el futuro. (Ver Anexo I)

3.2 Derecho a la limitación del tratamiento

En primer lugar cabe decir, a modo aclarativo, que el artículo 4 recoge la definición de limitación del tratamiento como "*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*". A su vez, este **nuevo derecho** recogido en el artículo 18 RGPC establece que: "*El interesado tendrá derecho a obtener del responsable del*

tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado."

Es decir, este derecho supone que bajo ciertas circunstancias, el responsable del tratamiento no puede cancelar ni tratar dichos datos.

Es el considerando 67 el que indica diferentes métodos a llevar a cabo por la organizaciones para lograr la limitación del tratamiento de datos como son: el traslado temporal de los datos seleccionados a otro sistema de tratamiento, el hecho de impedir el acceso de usuarios a los datos personales seleccionados o la retirada temporal de los datos publicados en un sitio web. Además, se debe indicar claramente en el fichero automatizado que los datos que se pretenden tratar se encuentran limitados para su tratamiento.

Este derecho necesita de un desarrollo nacional, donde se especifique diversas cuestiones como los plazos aplicables a cada uno de los supuestos o el procedimiento de ejercicio y respuesta del mismo.

3.3 Derecho a la portabilidad de los datos

Este **nuevo derecho** está recogido en el artículo 20 RGPD y reconoce la facultad del interesado a obtener los datos personales que le conciernan en un "*formato estructurado, de uso común y lectura mecánica*", que haya facilitado anteriormente al responsable, así como el derecho a que dicho responsable los transmita a un segundo responsable, cuando el tratamiento esté basado en el consentimiento o en un contrato y se realice por medios automatizados. En este sentido, el derecho a la portabilidad de los datos tiene dos

implicaciones: el interesado tiene tanto la facultad de recibir él mismo sus datos, como que el responsable los transmita a otro responsable sin que el primero se pueda negar a ello.

Asimismo, aunque el considerando 68 señala que "*debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de los datos*", el apartado 2 del artículo 20 establece que la transmisión directa entre responsables se realizará "*cuando sea técnicamente posible*", por lo que cuando se esgrima su imposibilidad el interesado quedará desprovisto de este derecho.

Otro problema que suscita este derecho es la falta de regulación relativa al plazo temporal que tienen los responsables del tratamiento para dar respuesta a las peticiones de portabilidad por parte de los interesados. Esto es, no se estipula el plazo que tienen los responsables para entregar los documentos con los datos al propio interesado o al responsable que éste designe. Además, cabe también señalar que, tal y como recoge el apartado 4 del referido artículo, el derecho a la portabilidad de los datos no se aplicará a las Administraciones Públicas.

Sin duda hay que resaltar que la aplicación de este derecho, siendo una gran oportunidad para todos los ciudadanos, supone grandes retos para los responsables que deben contar con plataformas interoperables. Las organizaciones deben invertir y adaptarse a los medios técnicos necesarios para hacer efectivo dicho derecho, aunque en el caso de transmitirlos a otro responsable, podrán ampararse en la imposibilidad técnica.

Con todo, podemos decir que el derecho a la portabilidad de los datos supone una mejora de la capacidad de control por parte los interesados sobre sus datos personales, pero ha quedado mermado o desvirtuado en su redacción final al hacer referencia a la viabilidad técnica. Por otro lado, deberá ser la norma nacional la que estipule el plazo que tiene el responsable para hacer efectivo ese derecho.

4. Obligaciones para las organizaciones

El desarrollo de este epígrafe se centrará en las obligaciones más relevantes y novedosas establecidas por el RGPD para el responsable del tratamiento y el encargado del tratamiento, siendo, en definitiva, las medidas que necesariamente deberán aplicarse en el seno de las empresas y autoridades y organismos públicos.

4.1 Protección de datos desde el diseño y por defecto

El modelo conceptual de la protección de datos desde el diseño (en inglés, *Privacy*[12] *by Design*) fue desarrollado por la Doctora Ann Cavoukian, Comisaria de Información y Protección de la Vida Privada de Ontario, Canadá (*Commissaire à l'information et à la protection de la vie privée de l'Ontario*) en los años 90 para abordar la evolución de las tecnologías, y desde entonces ha expandido la noción para incluir los procesos empresariales (Cavoukian, Taylor, & Abrams, 2010). Además, durante este tiempo, la Doctora Cavoukian ha colaborado con importantes multinacionales como IBM o Oracle para implementar su concepto.

Es decir, la protección de datos desde el diseño existe desde hace varias décadas, pero es ahora, en el artículo 25 del RGPD, que queda consagrado en un texto jurídico de tal magnitud, conjuntamente con la protección de datos por defecto. Se trata de dos medidas que tienen como finalidad cumplir los requisitos establecidos en el Reglamento y cuyo contenido supone importantes retos para las organizaciones como se puede comprobar en la Tabla 2. La protección de datos desde el diseño implica que la misma esté directamente integrada en la arquitectura del sistema informático y de la organización, utilizando, según el artículo 25, las "*medidas técnicas y organizativas apropiadas" y "teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento*".

Asimismo, la protección de datos por defecto supone que sólo serán tratados aquellos datos que sean necesarios para los fines para los que fueron recogidos y que será el interesado quien active la posibilidad de difusión de la información. Por ejemplo, al crearnos una cuenta en una red social, esta estará configurada de forma que sea el usuario quien decida activar su perfil público, el cual por defecto será privado.

Ambos conceptos tienen relevantes implicaciones puesto que ponen en relieve la necesidad de cambiar el desarrollo de la tecnología, y la importancia de concebir la tecnología no como una amenaza para la protección de los datos, sino como garante de la privacidad (*Privacy Enhancing Technologies,* PET) (van Blarkom, Borking, & Olk, 2003).

La Doctora Cavoukian establece 7 principios fundamentales y sus implicaciones, que serán brevemente expuestos en la siguiente tabla:

[12] El concepto de *privacy,* en este contexto, hace referencia a la necesidad de que las personas tengan control sobre sus datos personales.

Tabla 2. *Privacy by design: the 7 foundational principles*

PRINCIPIOS	CONTENIDO	IMPLICACIONES ORGANIZATIVAS
Protección proactiva y preventiva	No se trata de esperar la materialización de los riesgos ni de paliar los daños producidos, sino de prevenirlos. Debiendo así identificar las debilidades de los sistemas o aplicaciones.	Necesidad de un claro compromiso empresarial y creación de métodos para la detección temprana de diseños, prácticas y resultados deficientes en materia de privacidad
Privacidad por defecto	No se requiere la acción del usuario para proteger su privacidad, ésta forma parte del sistema. El interesado queda protegido automáticamente con los máximos estándares.	La finalidad de la captación, uso y conservación debe ser comunicada al interesado de forma clara y específica, debiéndose recoger sólo la información necesaria
Privacidad integrada en el diseño	La privacidad debe estar integrada en la arquitectura de los sistemas informáticos y las prácticas empresariales. Ya no se trata como un módulo accesorio, sino como un elemento nuclear.	Cuando sea posible, se ejecutarán evaluaciones de impacto, que serán publicados. En ellos se detallarán los riesgos observados y las medidas adoptadas para mitigarlos.
Funcionalidad plena "suma positiva", en vez de "suma cero"	Se pretende superar falsas dicotomías como privacidad vs seguridad, demostrando que se puede tener las dos, y que de hecho eso es lo deseable.	Diseñar sistemas en los que todos los intereses convivan. Se trata de no supeditar la seguridad, la funcionalidad o el beneficio empresarial a la privacidad.
Protección durante todo el ciclo de vida	Fuertes medidas de seguridad son esenciales para preservar la privacidad en todas las etapas. Se debe garantizar la confidencialidad, integridad y disponibilidad de los datos.	Se deben establecer protocolos de encriptación, métodos seguros de destrucción de datos, controles de acceso y registro y asumir la responsabilidad por la seguridad durante todo el ciclo de vida.
Visibilidad y transparencia	Son elementos clave para la responsabilidad proactiva y la confianza de los usuarios.	El contenido de las políticas y prácticas relativas al tratamiento deben ser públicas. La responsabilidad por los procedimientos debe ser comunicado y se debe señalar al responsable
Respeto por la vida privada del usuario	Empoderamiento de los usuarios; éstos deben tener un papel activo en la gestión de sus propios datos.	Debe estar apoyado por: - Consentimiento válidamente prestado - Calidad de la información: correcta, completa y actualizada - Acceso a los datos personales por sus interesados

Fuente: Adaptado y traducido de (Cavoukian, 2009)

4.2 Evaluación de impacto relativa a la protección de datos

Una evaluación de impacto relativa a la protección de datos personales (*Data Protection Impact Assessment*, en adelante DPIA) es una herramienta que analiza y gestiona los riesgos que puedan existir para la protección de datos de cualquier iniciativa (sistema de información, servicio, producto, proyecto, etc.) que implique el tratamiento de datos personales, con el fin de adoptar las medidas y controles necesarios para eliminar dichos riesgos o mitigarlos a niveles aceptables. Esta evaluación debe llevarse a cabo en una etapa inicial para que se pueda

influir en su resultado, realizando las correcciones oportunas para evitar los costes derivados de su descubrimiento cuando la iniciativa ya está en el mercado o en funcionamiento o cuando se ha lesionado el derecho a la protección de los datos personales. En estas situaciones, las organizaciones no sólo deberán hacer frente a costes económicos, sino también al daño de su reputación.

Las DPIA llevan décadas siendo utilizadas por países como Canadá, Estados Unidos, Reino Unido o Nueva Zelanda, y en los últimos años la AEPD ha promovido su implantación en España, aunque no fuese obligatorio, mediante una Guía sobre su importancia e instrucciones para llevarla a cabo.

Sin embargo, es ahora el RGPD quién regula la materia en el artículo 35 y establece su obligatoriedad en determinados casos. La evaluación de impacto se exigirá siempre que un tipo de tratamiento "*entrañe un alto riesgo para los derechos y libertades de las personas físicas*". Dada la falta de concreción de la noción "alto riesgo", el apartado 3 estipula tres situaciones donde será particularmente requerida una DPIA. Son las siguientes:

"a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público."

Existen términos como "sistemático" o "gran escala" que no quedan claramente delimitados. En este sentido, aunque haciendo referencia a artículos relacionados con la figura del Delegado de Protección de Datos, el WP29 ha clarificado estos términos (ver Tabla 3. Aclaraciones relativas al artículo 37.1 RGPD)

Tal y como establecen los apartados 4 y 5, la autoridad de control nacional de cada país, en el caso de España la AEPD, publicará una lista de los tipos de operaciones de tratamiento que requieran una DPIA y podrá también publicar una lista de los tipos de tratamiento que no requerirán dichas evaluaciones de impacto.

En cualquier caso, el artículo 35.7 hace referencia al contenido mínimo que la evaluación debe incluir: una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad y de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, así como las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Además el artículo 36 RGPD establece el deber de consulta del responsable a la autoridad de control antes de proceder al tratamiento si la DPIA concluye que el tratamiento va a suponer un alto riesgo si no se toman las medidas para mitigarlo.

Es, a su vez, importante señalar el papel que el artículo 35. 2 RGPD le otorga al Delegado de Protección de Datos, puesto que el responsable deberá recabar el asesoramiento de éste al realizar la evaluación de impacto.

4.3 Registro de las actividades de tratamiento

El artículo 30 RGPD (Ver Anexo II) establece esta obligación cuya finalidad es demostrar la conformidad con el propio Reglamento. El responsable y el encargado del tratamiento deberán llevar por escrito un registro de las actividades de tratamiento y de sus categorías, que contenga el nombre y los datos de contacto del responsable o del encargado, los fines del tratamiento, una descripción de las categorías de interesados y de las categorías de datos personales, las categorías de destinatarios a quienes se comunicarán los datos personales, las transferencias de datos personales a un tercer país o a una organización internacional y, cuando sea posible, contendrá también los plazos previstos para su supresión y una descripción general de las medidas técnicas y organizativa de seguridad.

A su vez, estos registros deberán ser puestos a disposición de las autoridades de control que lo soliciten, como herramienta de supervisión de las operaciones de tratamiento.

Siendo conscientes de la complejidad que entraña la llevanza de dichos registros, el mismo RGPD exime, en su artículo 30.5, de esta obligación a las organizaciones con una plantilla inferior a 250 trabajadores, "*a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías de*

datos especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10."

Es necesario subrayar que esta obligación de documentación no es responsabilidad del delegado de protección de datos, sino del encargado y del responsable del tratamiento.

Este registro, que debe contar necesariamente con el contenido anteriormente mencionado, es esencial para demostrar el cumplimiento del RGPD y supone que las organizaciones deban establecer los mecanismos necesarios para poder llevar dicho registro completo conforme al artículo 30.1 y 30.2

4.4 Violaciones de la seguridad de los datos personales

La definición de violación de la seguridad de los datos personales viene recogida en el artículo 4 y establece que se entenderá por tal, "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".

Son los artículos 33 y 34 los que hacen referencia a las acciones que se han de llevar a cabo tras una violación de la seguridad.

En primer lugar, el artículo 33 recoge la obligación del responsable del tratamiento de notificar a la autoridad de control la violación de la seguridad de los datos personales que haya tenido lugar, en un plazo máximo de 72 horas a contar desde que se haya tenido constancia de ella. Si la notificación se realiza pasadas las 72 horas, deberá incluirse un documento con los motivos de la dilación. Además, el responsable del tratamiento deberá documentar todas las violaciones de la seguridad de los datos personales. Por su parte, el artículo 33.2 establece la obligación del encargado del tratamiento de notificar al responsable las violaciones de la seguridad de las que tenga conocimiento.

El artículo 34.1 recoge que: "*Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida*", además el apartado 2 exige que dicha comunicación se realice "*en un lenguaje claro y sencillo*". Sin embargo, el artículo 34.3 establece tres excepciones, donde la comunicación al interesado no es necesaria si se cumple alguna de las condiciones siguientes:

- Cuando, tras la adopción de medidas de protección por parte del responsable, los datos sean inteligibles para cualquier persona que no esté autorizada.
- Cuando las medidas ulteriores tomadas por el responsable garanticen que ya no exista un alto riesgo para los derechos y libertades del interesado.
- Cuando suponga un esfuerzo desproporcionado. En tal caso se realizará una comunicación pública general para todos los interesados.

Además, el apartado 4 establece que para el caso de que "*el responsable no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.*"

Este es otro de los grandes retos y dificultades con los que se encontrarán las organizaciones, ya que en la actualidad éstas prefieren no dar a conocer sus problemas de seguridad informática para evitar daños a su imagen. Sin embargo, en esta nueva situación, deberán notificarlo obligatoriamente a la autoridad de control y en muchos casos a los interesados afectados, bajo pena de multa (ver epígrafe 4.6).

4.5 Códigos de conducta, certificaciones y sellos de seguridad

Los códigos de conducta y las certificaciones pueden ser usadas para demostrar el cumplimiento del RGPD, sin embargo, existen diferencias sutiles entre ambas y en el modo en el que son concebidas por la norma en los artículos 40 y 42 respectivamente. Cabe destacar que los códigos de conducta ya han sido recogidos en el artículo 27 de la Directiva 95/46/CE aunque ahora en el RGPD toman un papel fundamental. Por su parte, es la primera vez que se incluye un mecanismo de certificación como componente formal en la regulación del derecho a la protección de los catos personales.

Los códigos de conducta tienen como función facilitar la correcta aplicación del RGPD estableciendo marcos específicos de determinados tratamientos para los distintos sectores de actividad y las necesidades específicas de las PYMES y microempresas, de esta manera los responsables y los encargados del tratamiento podrán contar con guías prácticas, que les facilitarán el cumplimiento de sus obligaciones, garantizando los derechos de las personas. Los códigos de conducta serán elaborados en concertación directa con los organismos profesionales.

El establecimiento de mecanismos de certificación y sellos de calidad de protección de datos, permitirán a las personas evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios que serán ofrecidos por parte del responsable y del encargado del tratamiento.

A diferencia del código de conducta, el hecho de cumplir con los referenciales de una norma representa la voluntad del responsable o del encargado de cumplir con las disposiciones del RGPD, de esta manera, las certificaciones y los sellos de calidad se convertirán no sólo en una referencia, sino también en un elemento de distinción que promoverá la competitividad.

La adhesión a códigos de conducta o a certificaciones tiene los siguientes efectos comunes según el RGPD:

- Elemento para demostrar el cumplimiento de las obligaciones del responsable del tratamiento y del encargado del tratamiento (Artículos 24.3 y 28.5)
- Elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad (Artículo 32.3)
- Se tendrá en cuenta para la imposición de multas administrativas (Artículo 83.2.j.)

De forma separada, el mecanismo de certificación también será una herramienta que acredite el cumplimiento de las obligaciones relacionadas con la privacidad desde el diseño y por defecto (Artículo 25.3), y el cumplimiento de los códigos de conducta se tendrá en cuenta en las DPIAS (Artículo 35.8)

4.6 Multas administrativas, sanciones e indemnizaciones

El artículo 83 RGPD (ver Anexo II) recoge las condiciones para la imposición de **multas administrativas** y su cuantía, las cuales han de ser impuestas atendiendo cada caso concreto de forma proporcionada y con fines disuasorios.

Existen dos tipos de multas en función de la gravedad que son impuestas por las autoridades de control de cada Estado miembro. Según el artículo 83.4, se impondrá una cuantía máxima de 10 millones de euros o, "*tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la mayor cuantía*" cuando se infrinja alguno de los artículos relacionados con las obligaciones del responsable y del encargado (artículos 8,11,25 a 39,42 y 43), de los organismos de certificación (artículos 42 y 43) y de la autoridad de control (artículo 41.4).

A su vez, el artículo 83.5 establece que se sancionarán con multas administrativas de 20 millones de euros como máximo o, "*tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la mayor cuantía*" las infracciones relativas a los principios básicos para el tratamiento y al consentimiento (artículos 5,6,7 y 9), a los derechos de los interesados (artículos 12 a 22) y a las transferencias de datos personales a un destinatario en un tercer país o a una organización internacional (artículos 44 a 49), entre otras infracciones.

Además, es importante subrayar que el artículo 83.7 señala que cada Estado miembro tiene la facultad de decidir sobre la posibilidad de imponer dichas multas administrativas a las autoridades y organismos públicos establecidos en dicho Estado miembro. Cabe mencionar al respecto, que la actual LOPD en su artículo 46 relativo a las infracciones de las Administraciones públicas, excluye a las mismas de la imposición de las multas previstas en el artículo 45, que son únicamente aplicables a las empresas privadas, siendo su cuantía de entre 900 a 600.000 euros.

Haciendo referencia a las infracciones de las administraciones públicas, el artículo 83.9 recoge que "*Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control*."

Por otro lado, en cuestión de **sanciones**, el artículo 84.1 establece que: "*Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias*."

En lo relativo al **derecho a indemnización**, el artículo 82.1 prevé: "*Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos*." A su vez, el apartado 2 del artículo 82 establece que el responsable responderá de los daños y perjuicios causados por las operaciones que no cumplan con el Reglamento y que el encargado responderá únicamente

"*de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.*" Asimismo, el artículo 82.6 señala que "*las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro*."

Como se puede observar, este es otro ejemplo de la necesidad de un desarrollo nacional del Reglamento para establecer y delimitar el alcance exacto de las multas, sanciones y del derecho a indemnización.

En lo relativo a las administraciones públicas, aunque dependerá de cada Estado miembro que éstas puedan ser multadas por las autoridades de control, los Tribunales nacionales competentes (contencioso-administrativos) si podrán imponer multas con un efecto equivalente a las multas administrativas, tal y como establece el artículo 83.9. Además, los Estados miembros tienen la obligación de establecer otras sanciones aplicables distintas a las multas (artículo 84) y los particulares podrán ejercer su derecho a una indemnización ante los Tribunales (artículo 82.6)

En cuanto a las empresas privadas, las sanciones y el derecho a indemnización les afecta de la misma manera, y se les añadirá la posibilidad de recibir multas administrativas millonarias, mucho mayores de hasta las ahora establecidas por la LOPD.

V. ESPECIAL REFERENCIA A LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS

1. Semblanza histórica y terminología

Una de las novedades del Reglamento General de Protección de Datos es la obligatoriedad de la figura del Delegado de Protección de Datos (en inglés, *Data Protection Officer*, DPO) en ciertos supuestos. Esta figura es nueva en España pero tiene un largo recorrido en las Instituciones y Organismos de la Unión Europea, y también en ciertos países como Alemania, que fue el primer país en considerarla en su normativa nacional sobre protección de datos personales. La figura del '*Bundesbeauftragter für den Datenschutz*' fue incluida en el artículo 38 de Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz,* en adelante, BDSG), de 27 de enero de 1977.

Posteriormente, la figura del DPO, aunque no como la conocemos hoy, fue incluida en la Directiva 95/46/CE con el nombre de *Data Protection Official*. En la versión alemana mantuvo su nombre del BDSG de *Datenschutzbeauftragter* y en una traducción al español ciertamente liosa fue denominado "encargado de la protección de los datos", siendo muy similar a la de encargado de tratamiento (Ver Tabla 1. Sujetos relacionados con el tratamiento de los datos personales). Tanto en la versión inglesa como en la versión alemana la figura del DPO queda bien diferenciada del encargado de tratamiento, llamándose éste *processor* y *Auftragsverarbeiter*, respectivamente. En cuanto a las referencias a esta figura en la Directiva, es solamente mencionada en relación a la obligación de notificación a la autoridad de control (Artículo 18) y a los controles previos (Artículo 20) sin tener un papel importante.

En el marco de las Instituciones de la Unión Europea, el Reglamento (CE) 45/2001[13], recoge en el artículo 24.1 la **obligación** de designar un DPO para las instituciones y organismos comunitarios. Ya aquí en la versión inglesa se le denomina *Data Protection Officer,* en la alemana se mantiene como *Datenschutzbeauftragter* y en la española pasa a llamarse "responsable de la protección de los datos", volviéndose a una terminología poco adecuada por varias razones. La primera porque vuelve a ser muy similar a otra figura, a la del responsable del tratamiento, pudiendo ser confundidas. Y en segundo lugar tiene poca explicación que la misma figura sea primeramente llamada encargado bajo la Directiva 95/46/CE y posteriormente responsable por el Reglamento 45/2001, cuando las diferencias entre ambos son patentes.

Ahora, el RGPD denomina al DPO como «Delegado de Protección de Datos», que sin duda es una terminología mucho más acertada y cercana al significado de la noción en los otros idiomas. Sin embargo cabe destacar que mientras el término en alemán se ha mantenido intacto en los tres textos jurídicos, el inglés ha sufrido una pequeña modificación pero lleva desde 2001 siendo igual, el español ha cambiado en cada uno de los textos, lo que implica una inseguridad jurídica significativa.

La terminología con la que se hace referencia al DPO es fundamental en el RGPD, en especial en los casos donde su contratación sea voluntaria, puesto que desde el momento que se le denomine de esa manera en una organización, directamente implicará que se están cumpliendo todos los requisitos del Reglamento. Es decir, la denominación de DPO queda

[13] Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. (DO L 8 de 12.01.2011, p. 1-22).

exclusivamente reservada para aquellas organizaciones que desarrollen todos los mecanismos necesarios para cumplir con el Reglamento. De forma que la sociedad sepa con certeza y con todas las garantías que si cierta organización tiene un DPO es porque está cumpliendo con el RGPD, promoviendo así la seguridad jurídica al respecto. (Article 29 Working Party, 2016)

2. Definición

El artículo 4 del RGPD, relativo a las definiciones, donde la noción de responsable y de encargado del tratamiento, entre otras, están perfectamente señaladas podemos observar que falta la definición del DPO. A primera vista esta situación es confusa puesto que al ser una de las grandes novedades del Reglamento, debería estar claramente identificado. Sin embargo, una vez que se consideran los artículos 37, 38 y 39 relativos al Delegado de Protección de Datos, la ausencia de dicha definición se trata de una decisión consciente para evitar restringir quién puede ostentar dicho cargo.

En cualquier caso, el hecho de que no se restrinja quién pueda ser DPO no significa que pueda ser cualquiera. El artículo 37.5 del Reglamento establece el perfil que la figura del DPO requiere, en los siguientes términos: "*El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39*" y, a su vez, el considerando 97 señala que los conocimientos y aptitudes requeridas deben responder a las operaciones de tratamiento de datos que cada organización lleve a cabo, por lo que deberá atenderse a las características del tratamiento de datos de cada organización y no a criterios generales.

Para dotar a la figura del DPO con las máximas garantías y facilitar la contratación por las organizaciones, se establecerá un sistema de certificación que aseguren que estos profesionales reúnan los requisitos necesarios. Hay que resaltar que contar con esta certificación no será una condición para el acceso a la profesión, sino una manera de garantizar los conocimientos y aptitudes de los candidatos.

A pesar de que el RGPD deja abierto el abanico de los diferentes perfiles que pueda tener un DPO, existen razones por las que cabe plantearse que lo más adecuado sea que éste tenga un perfil jurídico. Nos encontramos ante un derecho fundamental que, especialmente en los casos en los que el tratamiento de los datos personales representa un riesgo para la persona, requiere tener una formación jurídica que permita evaluar el caso concreto y dar respuestas ante todas

las partes interesadas, ya sean el propio responsable o encargado del tratamiento, la autoridad de protección de datos u otras autoridades competentes. Aunque es también imprescindible tener conocimientos tecnológicos para entender la arquitectura de los sistemas, las vicisitudes de los tratamientos que se llevan a cabo y el contenido de las medidas que se pueden llevar a cabo, como la seudonimización o la encriptación, entre otras cuestiones.

En definitiva, dadas las funciones del DPO y el objetivo último del RGPD, sería preferible un perfil jurídico con conocimientos tecnológicos dado que se trata de asegurar la protección de "*los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*". Además de las habilidades profesionales, también es necesario que el DPO cuente con ciertas habilidades personales que favorezcan el desarrollo de sus funciones. De entre ellas podemos destacar: credibilidad, integridad, discreción, organización, asertividad y capacidad de comunicación y de negociación.

3. Designación

Como se mencionó anteriormente, lo verdaderamente novedoso de este Reglamento es el **carácter obligatorio** de la figura del DPO para las empresas públicas y en determinadas empresas privadas. Dicha obligatoriedad queda recogida en el artículo 37.1 del RGPD, con el contenido que a continuación se va a exponer.

En cuanto a los organismos públicos, se establece la obligación de contar con un Delegado de Protección de Datos para las autoridades u organismos públicos, salvo los tribunales cuando éstos actúen en el ejercicio de su función judicial. En cualquier caso, se recoge la posibilidad de que un conjunto de organismos disponga de un único DPO teniendo en cuenta su estructura organizativa y su tamaño.

En el caso de las empresas privadas, será obligatorio un DPO en dos situaciones: cuando "*las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una* ***observación habitual y sistemática de interesados a gran escala****" y para el caso de que "las actividades principales del responsable o del encargado consistan en el* ***tratamiento a gran escala de categorías especiales de datos personales*** *con arreglo al artículo 9 o de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.*"

En este artículo 37.1 existen multitud de términos cuyas definiciones no están determinadas y son fundamentales para delimitar los casos en los que existe la obligatoriedad de designar a

un DPO. Ante esta situación, el WP29 ha publicado una guía, llamada *Guidelines on Data Protection Officers ('DPOs'),* donde clarifica cuestiones de los artículos 37, 38 y 39 del RGPD, y entre ellas, establece el significado de estas nociones como se puede observar en la siguiente tabla.

Tabla 3. Aclaraciones relativas al artículo 37.1 RGPD

NOCIÓN	ACLARACIÓN
Autoridad u organismo público	Se incluyen las autoridades y organismos nacionales, regionales y locales. No se entenderá como tales aquellas empresas privadas que realicen servicios públicos (transporte, suministro de agua y luz, etc.), y, aunque en estos casos no sea obligatoria la designación de un DPO, se recomienda como buenas prácticas.
Actividades principales	Son aquellas necesarias para lograr los objetivos del encargado y responsable del tratamiento, donde el tratamiento de datos personales sea inherente a la actividad de ambos. Un ejemplo de ello son los hospitales, que no podrán llevar a cabo su labor de cuidado de pacientes sin tratar datos relativos a la salud, como el historial médico de los mismos.
Gran escala	No se puede establecer de forma cuantitativa lo que supone "gran escala". Sin embargo, se pueden considerar los siguientes factores: número o porcentaje de personas implicadas, el volumen de los datos y/o la variedad de tipos de datos, la duración del tratamiento o el alcance geográfico.
Observación habitual y sistemática	Se entenderá "habitual" cuando se de al menos una de las siguientes circunstancias: - Se lleve a cabo en ciertos intervalos para un periodo concreto - Se repita en momentos previamente fijados - Se realice de forma constante o periódica Será "sistemática" cuando se de al menos una de las siguientes circunstancias: - Ocurra en función a un sistema - Esté preestablecido, organizado o sea metódico - Sea parte de un plan general de recogida de datos - Se lleve a cabo como parte de una estrategia

Fuente: Adaptación y traducción (Article 29 Working Party, 2016)

A su vez, según el artículo 37.2 un grupo empresarial podrá contratar a un único DPO para todo el grupo, siempre y cuando, sea accesible desde cualquiera de los establecimientos del grupo empresarial. Cabe añadir, que para los casos en los que no sea obligatorio contar con la figura del DPO, las organizaciones que así lo consideren, podrán voluntariamente contratar uno. En este sentido, es muy importante recalcar que el DPO contratado en base a una decisión voluntaria debe cumplir el Reglamento de la misma manera que cuando éste sea obligatorio.

Además, queda establecido por el artículo 37.6 que el DPO puede ser contratado como trabajador dentro de la plantilla o ser un externo vinculado a través de un contrato de servicios.

4. Posición dentro de la estructura organizativa

La posición del DPO está recogida en el artículo 38 RGPD, que resalta por conformarse como una obligación impuesta tanto al responsable como al encargado de las cuestiones que serán desarrolladas a continuación.

El apartado 1 establece que: "*El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe* ***de forma adecuada*** *y* ***en tiempo oportuno*** *en* ***todas*** *las cuestiones relativas a la protección de datos personales*". Es fundamental que el DPO esté involucrado desde las primeras etapas de aquellas materias relacionadas con la protección de datos. Cabe destacar que esta pronta implicación del DPO en ocasiones es explícitamente mencionada por el Reglamento, como en el caso de las anteriormente señaladas evaluaciones de impacto relativas a la protección de datos recogidas en el artículo 35.2 RGPD.

A su vez, el artículo 38.2 recoge que: "*El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los* ***recursos necesarios*** *para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados*". Este artículo tiene un enorme impacto en las organizaciones que deban o quieran designar un DPO, debido en gran parte a la inversión económica que deberán realizar. Algunos de los recursos que deben prestar las organizaciones son (Article 29 Working Party, 2016):

- Apoyo activo por parte de la directiva.
- Respaldo adecuado relativo a recursos financieros, infraestructura y trabajadores
- Acceso a otros servicios, como al Departamento de Recursos Humanos, Departamento Legal o Departamento Tecnológico, con el fin de recibir ayuda e información.
- Formación continua.

Estos recursos deberán ser adaptados a cada situación empresarial como su tamaño o estructura. Además, cuanto más complejo y/o sensible sea el tratamiento, el DPO deberá poder contar con un mayor número de recursos.

Por último, el apartado 3 del artículo 38 estipula lo siguiente: "*El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba* ***ninguna instrucción*** *en lo que respecta al desempeño de dichas funciones.* ***No será destituido ni***

sancionado *por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos* ***rendirá cuentas*** *directamente al más alto nivel jerárquico del responsable o encargado*". Es decir, el DPO debe tener autonomía e independencia en el ejercicio de sus funciones sin que reciba directrices relativas a su papel como asesor sobre el cumplimiento del RGPD. Además, el hecho de que no pueda ser despedido ni sancionado por el responsable o por el encargado del tratamiento refuerza su independencia y asegura un nivel suficiente de protección a la hora de llevar a cabo sus tareas.

5. Funciones

El artículo 39.1 RGPD establece en los siguientes términos las funciones del DPO:

"1. El delegado de protección de datos tendrá ***como mínimo*** *las siguientes funciones:*

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto."

Cabe aquí destacar los apartados b) y c). En lo relativo al apartado b), y tal y como se verá en el siguiente epígrafe, es fundamental señalar que el hecho de que el DPO supervise el cumplimiento del Reglamento, no significa que sea responsable de los incumplimientos. A este respecto, se entiende por supervisión del cumplimiento llevar a cabo actividades relativas a identificar las actividades de tratamiento, analizar y comprobar su adecuación al RGPD

para, por último, informar sobre estas cuestiones al encargado y al responsable del tratamiento proporcionándoles asesoramiento y recomendaciones.

En cuanto al apartado c) relativo a la DPIA, el WP29 considera que el asesoramiento debe abarcar, entre otras cuestiones (Article 29 Working Party, 2016):

- La necesidad de llevar a cabo la evaluación.
- La metodología a seguir.
- Decidir si realizar la evaluación internamente o subcontratarla.
- Señalar las salvaguardias aplicables para mitigar posibles riesgos.
- Determinar si la evaluación se ha llevado a cabo correctamente y si sus conclusiones cumplen con el Reglamento.

En este sentido, en el caso de que el responsable del tratamiento no esté de acuerdo con la opinión del DPO, las razones que justifican esta discrepancia deberán constar en la documentación relativa a la evaluación de impacto.

Finalmente cabe resaltar que el WP29 recomienda que se precise claramente en el contrato del DPO el ámbito y las tareas específicas que éste ha de llevar a cabo.

A su vez, el artículo 39.2 recoge que: "*El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.*" Se trata de un enfoque basado en el riesgo que será fundamental en el desarrollo diario de las funciones del DPO, cuya finalidad es dar prioridad a aquellas operaciones de tratamiento que entrañen un mayor riesgo, para posteriormente establecer el foco en aquellas menos peligrosas.

6. Responsabilidad

Partiendo de lo establecido en el artículo 24.1 relativo a la «responsabilidad del responsable del tratamiento», "*el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*". Es decir, es el responsable del tratamiento y no el DPO, el responsable de los eventuales incumplimientos del Reglamento. En este sentido, el hecho de que el DPO tenga como función supervisar el cumplimiento del Reglamento, no significa que el DPO sea personalmente responsable en casos de incumplimiento.

En definitiva, el DPO es un asesor que dará su opinión en temas relativos a la protección de datos, y será el responsable o el encargado del tratamiento quien decida tomar en consideración o no la postura del DPO, aunque lo natural sería que actuaran conforme a lo estipulado por el DPO.

Es crucial resaltar que el cumplimiento de la normativa de protección de datos es una responsabilidad corporativa del responsable del tratamiento, no del delegado de protección de datos.

VII. CONCLUSIONES

En la actualidad debemos facilitar nuestros datos personales para poder disfrutar de cualquier actividad y/o servicio de la vida cotidiana. Buscar trabajo, abrir una cuenta bancaria, matricularse en la Universidad, pedir cita médica o usar aplicaciones móviles son sólo algunos ejemplos. Estamos absolutamente obligados a proveer nuestros datos personales si queremos llevar a cabo estas acciones. Pero, además, la situación se vuelve mucho más alarmante cuando nos damos cuenta de que, una vez entregados los datos, perdemos completamente el control sobre estos datos y la facultad para disponer y decidir sobre ellos.

Lo que pasa con estos datos ya es bien sabido por todos. Pueden ser directamente vendidos a terceros agentes o tratados por aquel que los recoge. En cualquier caso, son categorizados y tratados para establecer patrones y correlaciones que serán capaces de definir nuestro comportamiento, gustos o situación personal, esto es, para conocernos mejor que nosotros mismos. Luego, dicha información es utilizada para una multitud de fines para los que el conocimiento profundo y personalizado del individuo supone que las acciones que se lleven a cabo sean infinitamente más eficaces.

La revolución tecnológica está facilitando el menoscabo del derecho fundamental a la protección de los datos personales y, a su vez, ha dejado obsoleta el contenido de la actual regulación europea datada de 1995. Ante esta alarmante situación, las diferentes Instituciones de la Unión Europea han aunado esfuerzos, para poner fin a esta realidad, los cuales se han concretado con la publicación y entrada en vigor en 2016 del Reglamento General de Protección de Datos, que se aplicará en 2018.

El objetivo del presente Trabajo de Fin de Grado es recoger las novedades establecidas en el Reglamento, que dota de mayores garantías al referido derecho fundamental configurando

nuevos principios rectores, derechos de los ciudadanos y obligaciones para las organizaciones. Siendo de especial atención este último punto, en el que, a lo largo del documento, se recalca el impacto de la nueva regulación europea en las organizaciones, dándole una especial relevancia a la figura del Delegado de Protección de Datos y, asimismo, se indican posibles mecanismos y métodos para lograr el cumplimiento de la normativa europea.

Con el análisis del Reglamento, su comparación con la actual Directiva 95/46/CE y la revisión bibliográfica, ayudada por la experiencia adquirida durante las prácticas curriculares en el Supervisor Europeo de Protección de Datos, se ha pretendido reflejar el nuevo escenario que deben afrontar las organizaciones a partir de mayo de 2018. Aunque esa fecha parezca lejana, son muchas las acciones y medidas a tomar por las mismas y de gran calado, por lo que es necesario su progresiva implementación, puesto que requerirán de una gran inversión y una detallada planificación.

Cabe hacer aquí una especial mención al eje vertebrador de este Reglamento, el cual reside en la responsabilidad proactiva, la transparencia y en la protección de datos desde el diseño. Precisamente, este último es un ejemplo de que no tiene por qué existir obligatoriamente una confrontación entre la tecnología y el derecho fundamental a la protección de los datos. No es justificable que se desarrolle la tecnología a costa del derecho fundamental a la protección de los datos. Con ello, a la primera conclusión a la que debemos llegar es que la tecnología y la protección de datos no son enemigos *per se*. De hecho, podemos ir más allá, y señalar que precisamente es la tecnología la que puede conformarse como garante de la protección de datos, es decir, necesitamos de la propia tecnología para reforzar este derecho. Algunos ejemplos, además de la ya referida protección de datos desde el diseño, son la encriptación o la seudonimización.

Un segundo aspecto a recalcar es la verdadera función del Delegado de Protección de Datos, que actúa como un mero asesor en lo referente a las cuestiones relativas a la protección de datos. Esta consideración es crucial ya que ante incumplimiento del Reglamento, la persona que debe responder es, precisamente, el denominado responsable del tratamiento, figura la cual merecería de un estudio en profundidad en futuros trabajos.

Dejando por un momento a las organizaciones de lado, una tercera aportación relevante es el contenido y las implicaciones de la configuración de nuevos derechos para los ciudadanos, que, en definitiva, pretende otorgarnos un mayor nivel de protección y de refuerzo de este

derecho fundamental. Además, es importante señalar que la vulneración de estos derechos puede ser llevado a los tribunales, situación que conllevará un aumento de la litigiosidad considerable.

En definitiva, los ciudadanos debemos estar concienciados del valor de nuestros datos personales, de los usos fraudulentos que se pueden hacer con ellos y del peligro que supone que terceros tengan tanta información sobre nosotros. Se debe dejar de pensar en que la falsa idea de que al ser anónimos, nuestros datos no tienen valor. Es primordial que entendamos que en todos esos servicios gratuitos de los que hacemos uso en Internet, el producto somos nosotros. Y, también, es crucial que sepamos que uno de nuestros derechos fundamentales se está poniendo continuamente en jaque y que conozcamos su contenido y los modos de hacerlo valer.

Por su parte, las organizaciones deben también aumentar su nivel de sensibilización con este tema, donde la cultura de la protección de datos debe ser uno de los pilares fundamentales en el desarrollo de sus actividades. Además, el Reglamento contiene una serie de obligaciones, que afectan a toda la estructura organizativa y a todos los procesos donde se traten datos personales, a las que deberán hacer frente si no quieren que su imagen quede dañada además de recibir multas millonarias.

A su vez, cabe destacar que, el conocimiento por parte de los clientes de una mala gestión y uso de los datos personales por parte de las organizaciones, conllevará la pérdida de confianza de estos y podría repercutir negativamente tanto en la capacidad competitiva como en la imagen de la organización.

VII. REFERENCIAS BIBLIOGRÁFICAS

Alonso, C. (2016). You Are: Where You Are. Recuperado, el 28 de diciembre de 2016, de: https://www.youtube.com/watch?v=mMI_rYKPapU

Burgueño, P. (2015). Facebook ya tiene una ficha sobre ti, aunque no seas usuario la red social. Recuperado, el 31 de enero de 2017, de: http://www.pablofb.com/pabloburgueno.com/2015/06/facebook-tiene-una-ficha-de-tu-abuelo-aunque-el-no-sea-usuario/

Cavoukian, A. (2009). Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada*, 5. http://doi.org/10.1007/s12394-010-0062-y

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, *3*(2), 405–413. http://doi.org/10.1007/s12394-010-0053-z

Dumbill, E. (2012). *Planning for Big Data*. *O'Reilly Media, Inc.* http://doi.org/10.1017/CBO9781107415324.004

González Fuster, G., & Scherrer, A. (2015). *Big Data and smart devices and their impact on privacy*. Brussels. Recuperado de: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

López Aguilar, J. F. (2013). Por fin una ley europea de protección de datos (I). Recuperado, el 24 de diciembre de 2016, de: http://www.huffingtonpost.es/juan-fernando-lopez-aguilar/ley-europea-de-proteccion-de-datos_b_4148971.html

Maeztu, D. (2016). Nuevo reglamento europeo de protección de datos. Recuperado, el 1 de enero de 2017, de: http://tv.unir.net/videos/19809/0/Nuevo-reglamento-europeo-de-proteccion-de-datos---David-Maeztu

Palmer, M. (2006). Data is the New Oil. Recuperado, el 31 de enero de 2017, de: http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Rallo Lombarte, A. (2014). El derecho al olvido en el tiempo de internet: la experiencia española. *Percorsi Costituzionali 1.2014*, 159–192.

van Blarkom, G. W., Borking, J. J., & Olk, J. G. E. (2003). *Handbook of privacy and privacy-enhancing technologies*. *Privacy Incorporated Software Agent*. College bescherming persoonsgegevens. Recuperado de: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf%5Cnhttp://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf

FUENTES:

Agencia Española de Protección de Datos. (2004). *Guía del derecho fundamental a la protección de datos de carácter personal*. Madrid. Recuperado de: https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf

Article 29 Working Party. (2016). *Guidelines on Data Protection Officers* (16/EN WP243). *December*. Brussels. Recuperado de: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Supervisor Europeo de Protección de Datos. (2016). *EDPS launches Accountability Initiative*. Recuperado de: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-06-07_Accountability_factsheet_EN.pdf

LEGISLACIÓN:

Unión Europea. Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, L119, 4 de mayo de 2016, pp. 1-88.

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas*, L281, 23 de noviembre de 1995, pp. 31-50.

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, núm. 298.

BIBLIOGRAFÍA CONSULTADA:

Llaneza, P. (2010). Derechos fundamentales e Internet. *Revista Telos Cuadernos de Comunicación E Innovación*, *nº 85*, 54–57.

Rallo Lombarte, A. (2010). El derecho al olvido y su protección. *Revista Telos Cuadernos de Comunicación E Innovación*, *nº 85*, 104–108.

Ustaran, E. (2016). Data Protection Regulation: things you should know. *Privacy & Data Protection Journal*, *16*(3).

FUENTES CONSULTADAS:

Agencia Española de Protección de Datos. (2014). *Guía para una Evaluación de Impacto en la Protección de Datos Personales*. Recuperado de: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Deutsche Vereinigung für Datenschutz e.V. (2016). Rote Linien zur EU-DSGVO. Was ist daraus geworden ? *Datenschutz Nachrichten*, *39*(2/2016).

European Digital Rights. (2013). An Introduction to Data Protection, (6).

Supervisor Europeo de Protección de Datos. (2005). *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*.

Supervisor Europeo de Protección de Datos. (2015). *Dictamen 3 / 2015. La gran oportunidad de Europa*: *Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos*.

Supervisor Europeo de Protección de Datos. (2016). *Opinion 8/2016. EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*. Brussels.

Supervisor Europeo de Protección de Datos. (2016). *Opinion 9 / 2016. EDPS Opinion on Personal Information Management Systems Towards more user empowerment in managing and processing personal data*.

VIII. ANEXOS

Anexo I

ENTREVISTA CON JUAN FERNANDO LÓPEZ AGUILAR

1.- Teniendo en cuenta el largo proceso de negociaciones hasta llegar al Reglamento, me gustaría saber si usted está satisfecho con la redacción final.

"Para empezar, es cierto, el proceso de actualización del derecho europeo de protección de datos ha sido extremadamente prolongado, trabajoso y complicado. Arranca con la consternación, tras el lapsus de 10 años desde la aprobación de la antigua Directiva de Protección de Datos 95/46/CE, donde se ha producido una revolución tecnológica, que había hecho obsoletas muchas de las cláusulas reguladoras hasta entonces. Una revolución tecnológica que ha digitalizado la vida en todos sus ámbitos y la necesidad de que, además, la Unión Europea incorporase el mandato de la Carta de Derechos Fundamentales de la Unión Europea que, por primera vez en la historia, junto al Tratado de Lisboa protege la privacidad como un derecho fundamental de todos los europeos, el derecho a la vida privada, a la no interferencia de los poderes públicos. El derecho, por tanto, a lo que se denomina técnicamente la autodeterminación informativa, es decir, el control de la persona sobre el tratamiento automatizado de sus datos personales, después del esfuerzo que se emprendió por la anterior Comisión, la Comisión de Viviane Reding, siendo yo Presidente de la Comisión del LIBE, y, por tanto, de todo lo relativo al desarrollo legislativo de los derechos fundamentales de la Unión Europea. La legislatura entera se consumió con el anticipo de lo que luego ha sido, pues, la resistencia del Consejo, que es la reunión de los Gobiernos de los Estados Miembros, a adaptarse al Tratado de Lisboa, al carácter vinculante de los derechos fundamentales y aceptar plenamente el papel legislativo que ahora tiene el Parlamento Europeo. Hubo un encontronazo enorme entre la primera y la segunda lectura entre el Parlamento Europeo y el Consejo, que hizo que la legislatura anterior acabase sin haber completado el trabajo y que se haya completado, finalmente, en esta legislatura. Pero mi valoración es positiva, yo siempre subrayo que es la primera vez en la historia que el Parlamento Europeo prueba a ser además de legislador penal, que ya es un avance de gigante, legislador del desarrollo de derechos fundamentales de todos los europeos. Un Reglamento es una ley europea, el *Data Protection Regulation* es un Reglamento, es una ley europea, directamente vinculante para los Estados Miembros, y directamente invocable por los ciudadanos europeos ante Tribunales, que en buena medida desplaza el derecho interno de los

Estados Miembros en la materia, incluido el español que es una Ley Orgánica, que desarrolla un derecho fundamental del artículo 18 de la Constitución. Es un avance de gigante, luego están los elementos concretos, que son muy interesantes. Los elementos concretos son el reforzamiento del consentimiento, el derecho de acceso facilitado y también reforzado a los propios datos, el derecho al olvido condicionado y con sus límites pero que es un paso de gigante, que se ha ejercitado en España exitosamente contra Google. El *right to be forgotten* es algo muy importante. El incremento de la transparencia y el perfilamiento de algunos elementos de derechos subjetivos, como es el derecho de los padres a intervenir en el acceso de los menores a las redes y a los servidores y, en definitiva, a internet. Hay elementos también muy problemáticos como la llamada "*one stop solution*", que alude a que las compañías tengan derecho a acceder a una sola autoridad nacional de protección de datos, incluso cuando operan en distintos Estados Miembros, le permite un cierto *shopping*, de cual es la autoridad de datos nacional que sea más beneficiosa, la creación de una especie de consejo europeo de protección de datos, el *Data Protection Board*. Todo esto son elementos que claramente merecen una valoración positiva, de modo que, sin duda, el conjunto del derecho europeo a la protección de datos ha salido reforzado de esta experiencia y todo el mundo lo reconoce así, además cada vez cobra mayor importancia la jurisprudencia del Tribunal de Justicia que aplica directamente la Carta de Derechos Fundamentales de la Unión Europea como un parámetro de enjuiciamiento de todos los asuntos que llegan a su jurisdicción y la jurisprudencia del Tribunal de Justicia en materia de Protección de Datos es cada vez más relevante. Ha habido últimamente dos sentencias importantísimas en 2015, una la llamada *Digital Rights Ireland* y otra sobre el *Safe Harbor*, y otra la llamada sentencia *Schrems*, también sobre el *Safe Harbor*. La primera incidiendo sobre la anulación de la Directiva de protección de datos, por lo que son unas piezas legislativas de la mayor importancia. Mi valoración es positiva."

2.- Uno de los objetivos del Reglamento es conseguir o garantizar que el derecho a la protección de los datos sea lo más homogéneo posible dentro de la Unión Europea. ¿Cómo valora usted que el propio Reglamento de ese margen de maniobra a los Estados Miembros de a partir del Reglamento desarrollar leyes nacionales? Es decir, ¿esta situación no puede seguir fragmentando la aplicación homogénea de este derecho?

"En primer lugar, un Reglamento es directamente aplicable y directamente vinculante, no necesita transposición a diferencia de una Directiva. De hecho, parte del debate y de su dificultad consistió en sostener desde el Parlamento Europeo lo que habíamos identificado

como una estrategia de principio, un *Data Protection Package*, compuesto de dos piezas: un Reglamento directamente aplicable y vinculante para todos y una Directiva en lo relativo al manejo de datos personales en la lucha contra el delito, *law enforcement agencies*, contra el crimen (policía, judicatura, fiscalía). Esa es la llamada Directiva de protección de datos para *law enforcement purposes*, para propósitos de ejecución de la ley penal y de la lucha contra el delito. Pero el Reglamento que desarrolla el derecho fundamental de la privacidad, su contenido esencial y sus características en lo relativo al tratamiento automatizado de datos personales: transparencia, accesibilidad de los datos, control del procedimiento y de los datos personales, derecho a suprimir o corregir datos que te afecten o, en su caso, al olvido. Es decir, aquí un indexador o un servidor debe elimininar un determinado contenido en la medida que sea atentatorio contra la privacidad, que ya se está ejerciendo. Eso es un paso de gigante, y eso no necesita de desarrollo legislativo. Es un Reglamento directamente vinculante, el problema está en que de un tiempo a esta parte, los Estados Miembros vienen siendo cada vez menos europeístas. Sus gobiernos están en un repliegue nacional que hace que cada vez sean más frecuentes los casos de incumplimiento del derecho europeo y, por tanto, la necesidad de que haya una Comisión Europea fuerte, que se involucre en los llamados procedimientos de infracción ante el Tribunal de Justicia de la Unión Europea y les impongan sanciones fuertes. Ese es un problema ahora, el hecho de que muchos gobiernos están incumpliendo el derecho europeo, hay muchos gobiernos que están no solamente resistiendo a la integración europea sino incumpliendo el derecho europeo. Hay un ámbito que a mí me concierne por el manejo de los asuntos que llevo y es el ámbito de la mal llamada crisis migratoria, la mal llamada crisis de los refugiados, que es una crisis humanitaria de caballo, en la que los gobiernos incumplen el derecho europeo. Hace falta una Comisión fuerte para encarar eso, pero el Tribunal de Justicia está dictando sentencias que son claras, y si los Estados Miembro acataran las sentencias del Tribunal de Justicia el problema estaría resuelto, pero lamentablemente no es así."

3.- Usted ya ha mencionado aspectos relevantes de este Reglamento, como puede ser el derecho al olvido, la transparencia, el consentimiento, etc., y le quisiera preguntar sobre su valoración sobre el papel que puede jugar el Delegado de Protección de Datos o *Data Protection Officer*.

"Lo cierto es que se ha reforzado la obligación de quienes tienen el deber de vigilar por el cumplimiento de la regulación europea de la protección de datos en las empresas. Que incluye la designación, como tú has dicho de un *data protection officer*, y las compañías, es decir, las

empresas y corporaciones tienen ahora obligaciones reforzadas en relación con el cumplimiento del derecho europeo. Esto me parece bien, el papel que tiene cada uno de los componentes de este esquema es importante, incluidas las autoridades de protección de datos nacionales. Supuestamente, las autoridades nacionales tienen que equiparse mejor técnica y humanamente, es decir, recursos humanos, para asegurar el cumplimiento del derecho, y, en su caso, de los recursos interpuestos contra los incumplimientos. Supuestamente, el objetivo es reforzar el principio de responsabilidad corporativa (*accountability principle*), y en la medida en que las empresas sean capaces de hacer frente a este desafío de mejora en el cumplimiento del derecho europeo tendrán una mayor capacidad para competir a nivel global y para cumplir adecuadamente sus funciones respetando los derechos fundamentales involucrados. Este es un proceso en el que habrá que estar muy vigilante sobre cuál es su rendimiento durante el curso del tiempo. Pero la obligación de que las empresas designen delegados de protección de datos en sus estructuras parece que merece una valoración positiva."

4.- Teniendo en cuenta este largo proceso de negociaciones, me gustaría saber si al final usted ha echado en falta algún aspecto que debió o que se debió intentar incluir dentro del Reglamento.

"En el tiempo que llevo en el Parlamento Europeo, que ya suma siete años teniendo en cuenta la anterior legislatura y los dos de esta, he visto con claridad la complejidad a la que hay que habituarse. Los mecanismos de negociación son inevitablemente muy sofisticados y muy complejos, pero no hay que tenerle miedo a eso, hay que vivirlo minuto a minuto y llevarlos hasta el final. Y lo he visto en este caso. He solido señalar en mi experiencia que hay dos procedimientos legislativos que han desatado resistencias corporativas y empresariales de lo que se denominan habitualmente los *lobbys*, que operan ante la Unión Europea en mayúsculas, de dimensión estratosférica. Una fue la Directiva del tabaco y otra fue esta, el *Data Protection Package*. El *Data Protection Package* suscitó muchísima preocupación de los gigantes en la red: Google, Amazon, Facebook. Todos intentando aminorar el impacto de la nueva regulación para proteger sus intereses, y luego están las heterogeneidades nacionales. El resultado es satisfactorio, tanto es así que sobre la base de la nueva regulación, la Comisión ha interpuesto una multa descomunal. La Comisaria de Competencia, que se llama Vestager, ha interpuesto una multa tremebunda a Google por eludir sus beneficios en Europa residenciándolos en Irlanda. Una multa multimillonaria que significa, a mi juicio, una cierta fortaleza europea a la hora de embridar a los gigantes de la red, que de otro modo pueden

convertir los derechos fundamentales en papilla, es un riesgo muy serio. Aquí hay muchos intereses involucrados pero también derechos fundamentales, no sólo de los menores que son los más vulnerables y los más sensibles, muy permeables por la digitalización. Es decir, la pérdida de privacidad puede tener efectos devastadores en el derecho a la privacidad en los derechos fundamentales de los europeos en el futuro. Por tanto, creo que al final se consigue un equilibro razonable. Seguramente me hubiera gustado un mayor refuerzo del derecho al olvido, de hecho muchas veces que habría que darle el Premio Nobel de Economía o de la Paz, a partes iguales, a quien invente el modo de que internet no nos persiga toda la vida, y más allá de la muerte. En lugar de que toda tu vida quede ahí en una nube que cualquiera puede sacar y violar el derecho a la privacidad de cualquier ciudadano en cualquier momento. Esto es muy preocupante, desde el punto de vista de lo que es la teoría de los derechos fundamentales. El derecho al olvido, a mi juicio, debe ser reforzado, se consiguió para las personas que no tengan ningún perfil público, pero es sabido que todo el que tiene una participación en la vida pública soporta una especial vulnerabilidad, en lo relativo a la protección de su privacidad. Un derecho al olvido con todos los matices, que debió haber salido más fuerte. El derecho al olvido es un avance, y queda mucho por avanzar en su aseguramiento en el futuro."

Anexo II

ARTÍCULOS EXTRAÍDOS DEL RGPD REFERIDOS EN EL DOCUMENTO

Artículo 30

Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 83

Condiciones generales para la imposición de multas administrativas

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y

de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 99

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir del 25 de mayo de 2018.