SEGURIDAD VERSUS INTIMIDAD Y CIUDADANÍA; PAPEL DEL DELEGADO DE PROTECCIÓN DE DATOS Y RESPONSABILIDAD DE LAS INSTITUCIONES Y EMPRESAS EN EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS*

Lucas Andrés PÉREZ MARTÍN*

Sumario

1.- INTRODUCCIÓN

1.- El futuro debate sobre los conflictos internos en la Unión Europea en el ámbito del DIPr tendrá, con toda seguridad, una variante centrada en el derecho fundamental a la intimidad de sus ciudadanos concretado en especial en la protección de sus datos personales[1], la seguridad de los mismos, su borrado o su uso con fines comerciales[2]. En este marco nos parece esencial la figura del Delegado de protección de datos, *Data Protection Officer* (DPO en adelante), de las instituciones públicas y de las empresas que manejan habitualmente datos personales a gran escala, regulada en el Reglamento 2016/979, de 27 de abril de 2016[3], de tratamiento de datos personales (RPD en adelante). El RPD será aplicable a partir del 25 de mayo de 2018 –art. 99.2- y regulará en toda la Unión la protección de datos de los ciudadanos, la actividad de las autoridades de control, el régimen sancionador, y las acciones administrativas y civiles que pueden ejercitar los afectados para defender sus derechos[4].

---

* Esta contribución se ha finalizado en el transcurso de la estancia de investigación del autor en julio de 2017 como profesor visitante en el Departamento de Jurisprudencia de la Universidad de Torino, en el marco de una investigación centrada en la evolución del Derecho internacional privado europeo de familia y de la persona.

* Profesor Contratado Doctor Interino en la Universidad de Las Palmas de Gran Canaria (lucas.perez@ulpgc.es).

[1] Configurado el tratamiento de datos de los ciudadanos como Derecho Fundamental según los artículos 8 de la Carta de los Derechos Fundamentales de la UE, y 16.1 del Tratado de Funcionamiento de la UE.

[2] Como lo demuestra la trascendencia de las decisiones de la Comisión Europea al respecto en los últimos años o de las sentencias del TJUE, por ejemplo, por todas, el asunto *Google INC, AEPD, Costeja* (C-131/12, ECLI:EU:C:2014:317), ampliamente analizada por la doctrina.

[3] DO L núm. 119, de 4 de mayo de 2016, p. 1. El Reglamento deroga la Directiva 95/46/CE de 24 de octubre de 1995, DO L núm. 281, de 23 de noviembre de 1995, p. 31. Sobre la relación entre ambas normas y su necesaria evolución, véase, KOHLER, C., "Conflict of law issues in the 2016 data protecction regulation of the European Union, *RDIPP*, vol 3, 2016, pp. 653 a 675, p. 654. Otro interesante análisis sobre la evolución de la Directiva al Reglamento lo podemos encontrar en TAYLOR M., "Permissions and Prohibitions in Data Protecction Jurisdiction", *Brussels Privay Hub Working Papers*, mayo de 2016, vol 2, núm 6. Una visión más práctica de esta necesidad de evolución legislativa se puede apreciar en el comentario del Eurodiputado López Aguilar en http://www.huffingtonpost.es/juan-fernando-lopez-aguilar/ley-europea-de-proteccion-de-datos_b_4148971.html.

[4] Es evidente la gran trascendencia del cambio de instrumento legislativo adoptado por la Unión, sustituyendo una Directiva por un Reglamento. Al respecto, véase el apartado 3, pp. 7 a 10 de la Comunicación de la Comisión

2.- El RPD tiene como finalidad lograr una verdadera protección de los datos de los ciudadanos con residencia habitual en la Unión, uniforme y adaptada a los tiempos[5], y surge tras más de un lustro de complejos trabajos de las Instituciones europeas y los grupos de interés afectados[6]. En nuestra opinión, sus tres aspectos prácticos más interesantes son las obligaciones que impone a las empresas, la generalización en el Derecho europeo del DPO, y su régimen sancionador. Por ello, para analizar cómo el RPD podrá resolver en el futuro los conflictos surgidos en el derecho a la intimidad de los ciudadanos, en concreto en la protección de sus datos, aportaremos una inicial reflexión sobre su trascendencia y qué supone en la práctica, y de cómo podrá lograr la correcta aplicación del RDP y con ello evitar las posibles severas sanciones a las que se arriesgan las instituciones y empresas europeas a las que se les aplica.

2.- BREVE REFERENCIA A LOS ASPECTOS BÁSICOS DE DIPR EN EL REGLAMENTO DE PROTECCIÓN DE DATOS

3.- No podemos adentrarnos en la figura del DPO sin citar, al menos brevemente, los aspectos esenciales del RPD. Este se aplica al tratamiento total o parcialmente automatizado, o no automatizado, de datos personales contenidos o destinados a ser incluidos en un fichero, con intención comercial o no[7], siempre que el encargado o responsable de los datos tenga un establecimiento en la Unión[8], independientemente de que dicho tratamiento de datos tenga lugar en la Unión o no –art. 3.1-. Aunque en la actualidad no cabe afirmar la existencia de un marco regulatorio de la materia a nivel global, el RPD puede ser aplicado a establecimientos no radicados en la Unión si las actividades del mismo se dirigen a esta[9], sobre lo que volveremos al final del presente epígrafe.

Europea "*La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI"*, COM (2012), 9, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0009&from=ES. Todas las consultas realizadas el 14-7-17.

[5] A pesar de la "validez de los objetivos y principios de la Directiva" (Considerando 9 del RPD), el Reglamento acredita la necesidad de la evolución de la legislación europea al respecto (Considerandos 9 y 10).

[6] La Comunicación de la Comisión, COM (2010) 609, de 4 de noviembre de 2010, publicada en http://ec.europa.eu/health//sites/health/files/data_collection/docs/com_2010_0609_es.pdf, surgió a partir las consultas públicas que dieron lugar, entre otros, al documento del Grupo de trabajo del artículo 29 y de Grupo de Trabajo sobre Política y *Justicia "Furure of Privacy, Joint contribution to the Consultation of the European Comission on the legal framework for the fundamental right to protecction of personal data*", (02356/09/EN, WP 168), de 2009, disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[7] Art. 2.1 del RPD, señalando el art. 2.2 claramente que el mismo no se aplica, entre otras situaciones, al tratamiento de datos en investigaciones penales ni en las actividades exclusivamente personales o domésticas.

[8] Según el Considerando 22 un establecimiento estable implica "el ejercicio de manera efectiva y real de una actividad a través de modalidades estables", sin que la forma jurídica tenga trascendencia para ello.

[9] Establece el artículo 3.2 que se le aplicará el Reglamento a un responsable o encargado no establecido en la Unión si su oferta de bienes o servicios se hacen en la Unión, se pague por ellos o no, o si su comportamiento tiene lugar en la misma. Un estudio más detallado de cuándo se puede considerar que la actividad de la empresa se dirija

4.- En relación al RPD y a la actividad de las instituciones y empresas, debemos tener muy en cuenta que la responsabilidad para su aplicación y la tramitación de reclamaciones y la imposición de sanciones es de las autoridades administrativas de control de los Estados miembros, y no de una autoridad única de ámbito europeo –arts. 51 a 58-. El RPD comienza en su Capítulo II[10] estableciendo unos principios generales relacionados al tratamiento lícito de los datos, las condiciones para el consentimiento[11], o a los distintos tratamientos de los datos personales –arts. 5 a 11-. Define en el Capítulo III los derechos de los interesados, en concreto los derechos a la trasparencia, información, acceso, rectificación y supresión de sus datos o el derecho de oposición al tratamiento de sus datos, aplicables a partir de su entrada en vigor en toda la Unión – arts. 12 a 23-.

5.- Tras esto, en lo relativo a la competencia judicial internacional ante una lesión de sus derechos, el afectado se podrá dirigir o a la autoridad de control nacional vinculada a la publicación de esos datos[12] o a los Tribunales competentes de su residencia habitual, de su lugar de trabajo, del lugar de la supuesta infracción[13], o del Estado miembro en el que el responsable o encargado tenga un establecimiento[14]. Estas acciones serán las de solicitud de indemnización por los daños sufridos por el tratamiento de datos que vulnere la normativa aplicable a los mismos[15], siendo directamente aplicable a la reclamación los aspectos generales de

a la Unión –además de un amplio análisis de la competencia judicial y el derecho aplicable en el Reglamento-, lo podemos ver en DE MIGUEL ASENSIO, P. A., "Competencia y derecho aplicable en el Reglamento general sobre protección de datos en la Unión Europea", *REDI*, vol. 69, nº1/2017, enero-junio, pp. 75-108, p. 83 a 86.

[10] Tras unos extensos 173 considerandos que acreditan la complejidad técnica del RPD y el habitual Capítulo I que estable el objeto, ámbito de aplicación material, territorial y las definiciones –art. 1 a 4-.

[11] El artículo 8 establece el único ámbito material en el que el RPD permite a los Estados regular de forma diferente alguno de sus aspectos. En concreto la posibilidad de establecer en los menores de edad una edad inferior a los 16 años para expresar el consentimiento en el tratamiento de sus datos por sí mismo, sin que el consentimiento lo otorgue quien ejerza la patria potestad, limitándolo en todo caso como mínimo a la edad de 13 años.

[12] Artículos 55 a 58, estableciendo el artículo 56 los criterios para establecer cuál se debe considerar autoridad de control principal en los supuestos de un tratamiento de datos por un responsable en varios Estados de la Unión. Destacamos que todo un Capítulo, el VII, regula en los artículos 60 a 76 la cooperación y coherencia en la actuación de las diversas autoridades intervinientes y crea incluso un novedoso Comité europeo de protección de datos.

[13] Artículo 77.1 para las reclamaciones ante las autoridades de control y 79.2 en las reclamaciones judiciales. En una clara línea continuista con los últimos Reglamentos aprobados por la Unión, como los reguladores del derecho de alimentos, sucesiones o regímenes económicos matrimoniales y de uniones registradas, el primer criterio aplicable a falta de acuerdo entre las partes es el de la residencia habitual del afectado. Respecto al concepto de residencia habitual en el ámbito de la protección de datos, se puede entender más extenso que el habitual concepto jurisprudencial del "centro de vida y de intereses" (ver por todas, la clásica STJUE de 15 de septiembre de 1994, C-452/94, ECLI:EU:C:1994:332, *caso Magdalena*, apartado 22), debiendo tener en cuenta otros criterios, como el del ejercicio de una actividad profesional, todo ello a tenor del contenido de la STUE, de 25 de octubre de 2011, C-509/09, ECLI:EU:C:2011:685 *eDate Advertisinh y Martínez*, apartado 49.

[14] Salvo en el supuesto en el que "el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en el ejercicio de sus poderes públicos", en cuyo caso la demanda se debe interponer ante los Tribunales del citado Estado en todo caso, art. 79.2 del RPD.

[15] Artículo 79.2 del RPD, así como evidentemente para el ejercicio del resto de los derechos reconocidos por el mismo, como la rectificación, supresión o limitación o prohibición de tratamiento de los datos del afectado.

competencia judicial del Reglamento Bruselas I bis, sin que la protección de datos se encuentre entre una de las materias excluidas del mismo.

6.- Sobre la ley aplicable, el RPD, como ya hemos citado, será directamente aplicable en todos los procedimientos seguidos en un Estado de la Unión, incluso ante posibles infracciones del mismo ocurridas con origen en un Estado externo –art. 3-. Y en el análisis de las consecuencias indemnizatorias de la posible vulneración de un derecho contenido en el RPD, se deberá tener en cuenta si la misma surge de un contrato, en cuyo caso se aplicará la norma de un Estado según las prescripciones establecidas en el Reglamento Roma I, o de una relación extracontractual, en la que no es aplicable el Reglamento Roma II[16]. Finalmente dejamos únicamente apuntado que esta posible aplicación del RPD a empresas radicadas fuera de la UE provocará en el futuro, creemos, un gran debate doctrinal, ya iniciado, y una natural polémica sobre la dimensión internacional del RPD, su aplicación extraterritorial, y las posibles responsabilidades de entidades con domicilio fuera de la Unión[17].

3.- EL DELEGADO DE PROTECCIÓN DE DATOS, OBLIGATORIEDAD, COMPETENCIAS, TRASCENDENCIA

7.- Es de sobra conocida la importancia que tiene en la actualidad el procesamiento masivo de datos para grandes corporaciones e instituciones públicas, su valor económico y su actual situación de falta de control global[18], tanto en España como en el resto de la Unión[19]. Y este

[16] En el primer supuesto, aplicable el artículo 6 del Reglamento Roma I, se aplicará la ley acordada en el contrato, si bien el consumidor afectado podrá solicitar la aplicación de las normas de protección de consumidores de su residencia habitual más favorables a las acordadas en el contrato. En el caso de un daño de origen extracontractual, el artículo 1.2.g del Reglamento Roma II establece que el mismo no es aplicable a la difamación relacionada con los derechos de la personalidad, debiendo acudir a las normas de conflictos establecidas en Tratados Internacionales o en la normativa interna –en España el art. 10.9 del CC-. Al respecto nos remitimos al citado estudio del profesor DE MIGUEL ASENSIO P. M., "Competencia y derecho…", *op. cit*. nota 9, p. 104 a 106.

[17] Un interesantísimo trabajo analizando el alcance y los efectos extraterritoriales del RPD lo encontramos en KUNER. C., "Extraterritoriality and regulation of international data transfer in EU data protection law", *IDPL*, vol 5, nº 4, pp. 235-245. También se puede ver una propuesta de *lege ferenda* al respecto en BRKAN, M., "Data Protection an European Private Internacional Law", *Robert Schuman Center for advanced Studies Research Paper* n. *RSCAS 2015/40*, july 2015, pp. 34 a 36.

[18] Falta de control que ha provocado los procedimientos sancionadores conocidos que aquí hemos citado, con indemnizaciones millonarias algunos de ellos. Muchos son los trabajos que han analizado los *Big Data* y su trascendencia económica en el futuro como nueva fuente de recursos económicos y sector de negocios, entre los que podemos citar, por ejemplo, a DUMBILL, E., *Planning for Big Data*, Sebastopol, Primera edición, O´Reilly Media, 2012, Inc, pp. 47 a 71. Esta trascendencia se aprecia, cómo no, en los interesantes dictámenes del Comité Económico y Social Europeo (DO C núm. 229, de 30 de julio de 2012, p. 90) y del Comité de las Regiones (DO C núm. 291, de 18 de diciembre 2012, p. 127) durante la tramitación legislativa del RPD. Un interesante trabajo que analiza globalmente la violación del derecho a la intimidad en los negocios internacionales es el de SANCHO VILLA, D., *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010.

[19] Importancia que se aprecia en los trabajos españoles y anglosajones ya citados, y por ejemplo en la doctrina italiana en su análisis desde distintos puntos de este tema en los recientes trabajos de DAL POZZO, F. R., "La

hecho motiva que para la adecuada protección del derecho a la intimidad, en su vertiente del procesamiento de los datos, el control de los mismos sea esencial y necesite la actuación de una figura técnica, profesional, y en todo caso independiente del resto de poderes económicos de la empresa. Para ello el RPD generaliza la figura del DPO para determinado tipo de sociedades e instituciones, lo que exigirá a las empresas e instituciones una proactiva y costosa adaptación de sus estructuras, políticas y cultura empresarial hasta la entrada en vigor del RPD el 25 de mayo de 2018.

8.- El RPD no aporta una definición del DPO, al contrario que sí lo hace con otros sujetos que regula[20]. Esta figura tiene una tradición de largo recorrido en algunos países de la Unión Europea, como Alemania, y en las Instituciones de la propia Unión, pero es desconocida tanto en España como en otros Estados, en especial del sur de Europa[21]. El artículo 37.5 establece la cualificación que debe tener el DPO, en concreto "conocimientos especializados en Derecho y la práctica en materia de protección de datos"[22], señalando también la necesidad de tener capacidad para "desempeñar las funciones del artículo 39", para nosotros en una clara confirmación del liderazgo, autonomía e independencia con la que ha de trabajar el DPO.

9.- El artículo 37.1 establece la obligatoriedad del nombramiento del DPO en las empresas e instituciones que se encuentren en los siguientes supuestos; 1.- Cuando una autoridad u

tutela di dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona", *RDI*, vol 3, 2016, pp. 691 a 724, o DAL POZZO, F. R., "Protezione dei dati personi e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione", *RIDIPP*, vol 4, 2016, pp. 1021 a 1059.

[20] El artículo 4 define al "responsable del tratamiento" o "responsable" (núm. 7), al "encargado del tratamiento" o "encargado" (núm. 8), al "destinatario" (núm. 9), e incluso al "tercero" (núm. 10). Como vemos, tampoco se regula una específica definición del "titular" de los datos personales afectado por la vulneración de sus derechos. Un interesante trabajo global sobre el derecho europeo de protección de datos podemos consultarlo en BOLLIAT, F. y KJAERUM, M., *Manual de legislación europea en materia de la protección de datos*, Luxemburgo, Primera edición, Oficina de Publicaciones de la Unión Europea, 2014, pp. 13 a 198.

[21] En Alemania desde la regulación de la figura del *"Bundesbeauftragter für den Datenschutz"* incluida en el artículo 38 de la Ley Federal de Protección de Datos de 27 de enero de 1977, y en la actualidad regulado en la sección 4f de la Ley Federal de Protección de Datos de 20 de diciembre de 1990. En la Unión Europea se prevé la posibilidad para los Estados desde que la presión alemana precisamente provocase su inclusión en el artículo 18.2 de la Directiva 95/46/CE, que preveía la designación "con arreglo al derecho nacional" de un "encargado de protección de los datos personales", *"Data Protection Official"*, o en la traducción alemana manteniendo el nombre de *"Datenschutzbeauftragter"*. Al limitarse al derecho nacional solo se implantó en los Estados que ya la regulaban. Las Instituciones europeas incluyeron dicha figura a partir de la aprobación del Reglamento (CE) 45/2001 (DO L 8, de 12 de enero de 2001, p. 1) que en su artículo 24.1 lo establece como obligatorio (Considerando 32, arts. 24 y 25 y Anexo). Como vemos, es el claro antecedente del DPO. Sobre la situación actual del DPO en toda Europa, véase el interesantísimo, por original en su extensión, trabajo de SEMPERE SAMANIEGO, J. *Comentarios prácticos a la propuesta de Reglamento de protección de datos de la Unión Europea*, Licencia creative commons, 2013, p. 337, dedicando al DPO el Capítulo 11, pp. 335-359.

[22] Desde luego en una falta de concreción muy criticable a nuestro juicio, ya que no se concreta el nivel de conocimientos de derecho o de práctica en la materia de protección de datos que debe tener el DPO y este es un aspecto absolutamente esencial. Por ejemplo, ¿es necesario que sea Graduado en Derecho, será válido un curso de especialización? No creemos que sea un aspecto a dejar desarrollar por la Jurisprudencia.

organismo público lleve a cabo el tratamiento de los datos[23]; 2.- Cuando la actividad principal de la empresa suponga el tratamiento de datos que requieran una observación habitual y sistemática de datos de interesados a gran escala; 3.- Cuando se produzca un tratamiento a gran escala de categorías especiales de datos, como los médicos o privados[24]. Desde luego podemos apreciar una gran indeterminación, lo que provocó que el Grupo de Trabajo del artículo 29 WP29 estableciese en la importantísima guía "*Guidelines on Data Protection Officers"* qué se entiende por autoridad u organismo público, actividad principal, gran escala u observación habitual y sistemática[25]. Aun así, a falta de una futura determinación por las autoridades de control y por la Jurisprudencia de qué instituciones y empresas estarán obligadas a contar con un DPO, se puede indicar sin temor al error que el número de instituciones obligadas será numeroso, y en todo caso lo estarán las grandes empresas cuyo objeto sea el comercio a una escala significativa, las instituciones públicas, así como todas las PYMES con una actividad que tenga relación con datos médicos o privados de las personas, pudiendo ser nombrado un DPO para grupos empresariales o administraciones, pudiendo ser contratado o subcontratado[26].

10.- Consideramos esencial detenernos en el estatus del DPO en la empresa. Incluso el RPD regula antes, en su artículo 38, esta posición, que sus funciones, contenidas en su artículo 39, ya que su independencia, influencia y liderazgo condicionan el ejercicio de sus funciones. Consideramos que su característica esencial es la establecida en el apartado tercero que exige

[23] Salvo el caso de los Tribunales que actúen en el ejercicio de su función judicial en la intención de proteger dicho ejercicio. No consideramos dicha excepción imprescindible y dejamos indicado que dudamos de su oportunidad. Consideramos que será debatido en el futuro si todas las administraciones públicas, por grandes o pequeñas que sean, deberán tener cada una de ellas un DPO independiente (pensemos en pequeños municipios de unos pocos habitantes, por ejemplo), o si el mismo se podrá agrupar entre diversas pequeñas administraciones según su configuración (uno por islas para los municipios de menos de x habitantes, por ejemplo, en Canarias o Baleares).

[24] En concreto dentro de estos tipos de datos especiales se encuentran, enumerados en el art. 9, los datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos genéticos o biométricos, de la salud o de la vida u orientación sexual de las personas. El artículo 10 cita en esta categoría las infracciones o condenas penales.

[25] Documento del Grupo de trabajo del artículo 29 "*Guidelines on Data Protection Officers (DPOs)"*, (16/EN, WP 243.rev.01), acordado el 13 de diciembre de 2016, revisado el reciente 5 de abril de 2017, pp. 5 a 9, disponible en https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf. El nombre del Grupo de trabajo surge de su regulación y creación en el artículo 29 de la Directiva 95/46/CE.

[26] Art. 37, apartados 2 a 4 en el caso de instituciones o empresas colecticas, y apartado 6 y 7 en su régimen jurídico y comunicación pública. Los primeros borradores del RPD establecían un periodo mínimo de nombramiento de del DPO de dos años y que las empresas con más de 250 trabajadores tendrían obligación de tener un DPO, dos obligaciones que el documento finalmente aprobado no contempla en su texto. Algunos trabajos han debatido sobre este hecho, en especial sobre la obligación en empresas de más de 250 trabajadores, como el de DIAZ DIAZ, E., "El Data Protection Officer en el nuevo Reglamento de Protección de datos", *ELDERECHO.COM*, 25-4-2016, consulta en, http://tecnologia.elderecho.com/tecnologia/privacidad/Protection-Officer-DPO-Reglamento-Proteccion-Datos-UE_11_945055002.html. Finalmente, el artículo 30.5 sí que limita algunas de sus obligaciones a empresas de menos de 250 trabajadores. En todo caso, dada la naturaleza del DPO, si la empresa supera ese número de trabajadores lo hace en todo caso muy aconsejable y necesario, si bien no legalmente obligatorio. Es muy importante destacar que las empresas o instituciones no obligadas a tener un DPO pueden nombrarlo, el RPD no lo prohíbe, y consideramos que sus objetivos lo aconsejan, pero para que produzca los efectos positivos para la organización que prevé y aquí citaremos debe cumplir todas las obligaciones que el mismo establece.

una absoluta independencia, y que no pueda recibir "ninguna instrucción" del responsable y del encargado del tratamiento, y que "no será destituido ni sancionado por el responsable o encargado por desempeñar sus funciones", rindiendo cuentas "directamente al más alto nivel jerárquico del responsable o del encargado". Como podemos entender, será una figura trascendental, que tendrá un estatus jurídico ciertamente privilegiado, pero una situación difícil, cuanto menos delicada,[27]. Para poder llevar a cabo dicha función el DPO deberá contar con los recursos necesarios para ello, lo que supondrá una exigencia de inversión que no todas las entidades pueden estar preparadas para asumir[28].

11.- En relación a las funciones del DPO recogidas en el art. 39 del RPD. Cinco son las funciones esenciales; 1.- Informar al responsable, al encargado del tratamiento y a los empleados afectados de las obligaciones que impone el RPD; 2.- Supervisar del cumplimiento de toda la normativa europea y estatal de la protección de datos, la asignación de responsabilidades, la concienciación y formación del personal; 3.- Informar expresamente sobre la evaluación de impacto regulada en el art. 35[29]; 4.- Cooperar con la autoridad de control; 5.- Actuar como punto de contacto con la autoridad de control, en especial en las situaciones de consulta previa. Como vemos estamos ante un grupo de funciones claramente dual que también podrá provocar situaciones conflictivas en el futuro. Por un lado, las tres primeras funciones las debe desempeñar directamente dentro de la empresa, tanto con el responsable y el encargado

[27] Desde luego no podemos entrar en el desarrollo de la totalidad de aristas de esta difícil situación en un breve trabajo como es el presente, pero son muchas las cuestiones que el futuro deberá responder, en especial en Estados como España que no tiene una gran tradición de este tipo de figuras que provienen del mundo anglosajón (al igual que ocurre en el ámbito penal con el responsable de cumplimiento normativo o *"Compliance officer"* introducido en el artículo 31 bis 2 del Código Penal por la LO 1/2015, de 30 de marzo, por la que se modifica el Código Penal, BOE 1 de julio de 2015). Consideramos que los conflictos pueden ser muchos, y desde dos perspectivas. Primero, desde la perspectiva de existir problemas en el actuar del DPO, ¿Qué ocurrirá, dada esta regulación, si una vez nombrado, y en el ejercicio de sus funciones, se aprecia que el DPO no lleva a cabo un correcto asesoramiento de la empresa? ¿O si hace dejación de funciones? ¿O si propone medidas desproporcionadas y lesivas para la empresa? Segundo, desde la perspectiva de un incorrecto actuar de la institución, ¿Cómo puede reaccionar el DPO si no recibe los recursos suficientes? ¿Y si la preparación del resto del personal no es adecuada y la empresa no los forma? ¿Y si en el desempeño de su trabajo no se le da acceso a los medios o personal que necesita o la persona de más alto nivel jerárquico? Y por supuesto, si es despedido por causas vinculadas al desempeño de su función, pero disfrazadas de causas terceras, ¿qué ocurrirá con la función en el periodo transitorio de esta situación? Véase, al respecto, la inicial reflexión que realiza el Grupo de trabajo del artículo 29 citado, "*Guidelines on Data Protection Officers (DPOs)", op. cit*. nota 24, pp. 14 y 15.

[28] El documento del Grupo de trabajo del artículo 29 citado, "*Guidelines on Data Protection Officers (DPOs)", op. cit*. nota 24, p. 14, hace un somero repaso de los recursos que necesitará el DPO, que variarán de empresa a empresa, según su configuración, pero que en todo caso deberán ser, apoyo general, tiempo suficiente para realizar su trabajo, recursos financieros, infraestructuras y trabajadores a su cargo, si fuesen necesarios. Por supuesto acceso a otros servicios de la organización y una formación continua.

[29] No podemos detenernos en la misma, pero señalaremos que se trata de una evaluación del impacto de las operaciones de tratamiento de la protección de datos que debe realizar la empresa cuando se utilice nuevas tecnologías o supone un tipo de tratamiento de alto riesgo para los derechos o libertades de las personas físicas.

del tratamiento, como con sus empleados[30]. Pero también tiene función de contacto, relación, ayuda y cooperación con la autoridad de control en el momento de la realización de cualquier comprobación respecto al tratamiento de datos en la empresa[31].

12.- La trascendencia de la figura del DPO obliga, de ahora al 28 de mayo de 2018, desde luego, a una adaptación de las empresas a su presencia, competencias, poder y especial régimen para poder cumplir fielmente con el RPD. Un somero repaso a las webs públicas de grandes empresas o despachos de abogados que trabajan en el ámbito mercantil nos permite apreciar que la figura y el Reglamento han provocado mucha difusión de información sobre la importancia del DPO, y evidentemente el surgimiento de formación especializada sobre el mismo, e incluso una certificación pública por parte de la AEPD[32].

4.- RESPONSABILIDADES ECONÓMICAS DE LAS INSTITUCIONES Y EMPRESAS EN EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS

13.- No podemos finalizar este estudio sin hacer una referencia al severo régimen sancionador administrativo que establece el RPD. Por un lado, ya señalamos que los ciudadanos pueden acudir a los Tribunales a solicitar la restitución en sus derechos dañados mediante la solicitud de indemnización de daños y perjuicios[33]. Pero, de forma simultánea a esta acción, las autoridades de control podarán imponer sanciones a las empresas que no cumplan con las obligaciones que establece el RPD, acorde a la naturaleza, gravedad y duración de la infracción. Estas sanciones, según su articulado, serán graduadas, pueden –y en nuestra opinión, deben-,

[30] Es muy importante destacar que, a tenor del artículo 24.1 del RPD, el responsable frente a terceros de su falta de aplicación no es ni el encargado del tratamiento, ni el DPO, sino que lo es el responsable del tratamiento de datos de la institución, por lo que al DPO no puede declarársele responsable del tratamiento erróneo de los datos.

[31] Es una situación que en principio puede parecer algo contradictoria y confusa, pero desde luego que el DPO, figura encargada de hacer cumplir el RPD y por lo tanto conocedora del mismo, será el más indicado para resolver cualquier duda de la autoridad de control o ayudarla a conocer mejor las actividades desarrolladas por la empresa. Desde luego que en dicha situación seguirá debiendo ser considerado principalmente un empleado de la empresa y por ello vinculado a ella, pero con una función de colaboración con la administración.

[32] El art. 39.5 del RPD habla expresamente de sus conocimientos en Derecho y la práctica en la materia de protección de datos. Al respecto la AEPD, en colaboración en la ENAC (Entidad Nacional de Acreditación), presentó el reciente 13 de julio de 2017 el esquema de certificación de acreditación de Delegados de Protección de Datos que aportará seguridad y fiabilidad a la figura, permitiendo la homologación de su formación. Véase en https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Certificacion/ESQUEMA_AEPD_DPD_PUBLICO_1.0.pdf. Hasta este momento existían dos certificados otorgados por asociaciones profesionales privadas españolas. Al respecto, véase a SEMPERE SAMANIEGO, J. *Comentarios prácticos a la propuesta de Reglamento de protección de datos de la Unión Europea*, *op. cit*. nota 21, pp. 354 y 335, que también recoge la existencia de la Confederación Europea de DPO con organizaciones francesas, alemanas y holandesas en su seno.

[33] Acción prevista en el artículo 82 del RPD.

ser rebajadas si la actuación del DPO ha sido acorde a las obligaciones del RPD y puesta en práctica por la empresa, y de ahí su inmensa importancia en la organización[34].

14.- Estas sanciones son muy serias. Si se han vulnerado los artículos relacionados con las obligaciones del responsable y del encargado[35], o las obligaciones de los organismos de certificación[36], o las obligaciones de la autoridad de control[37], se impondrá una multa administrativa de 10 millones de Euros 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. Y si se han vulnerado los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento[38], los derechos de los interesados[39], o las trasferencias de datos a un destinatario de un tercer país[40], entre otras, se impondrá una multa administrativa 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 de mayor cuantía.

5.- CONCLUSIONES, REFLEXIÓN SOBRE EL FUTURO DEL DPO Y LA RESPONSABILIDAD DE LAS EMPRESAS

15.- El RPD regulará la protección del Derecho fundamental al tratamiento de los datos de los ciudadanos europeos a partir del 28 de mayo de 2018. Fija la competencia para el inicio de las acciones en los lugares de residencia habitual del afectado, el lugar de su trabajo habitual, en el lugar de la lesión, o el domicilio de la empresa o institución. En él el DPO se convierte en una figura esencial, tanto para proteger el Derecho fundamental de los ciudadanos a la protección de datos, como para legitimar la actuación de las empresas, así como, finalmente, para protegerlas de las graves consecuencias económicas que el RPD puede suponerles. Su función esencial es la de asesorar a la empresa o institución en la correcta aplicación del RPD, sin ser

[34] El artículo 83 se detiene de forma detallada a establecer cuáles son los criterios que se deben tener en cuenta, destacando el propósito de la acción, la intencionalidad o negligencia para imponer la sanción –letras a a e-. Sin embargo, también establece en las letras f a j que la sanción se podrá graduar valorando las medidas tomadas para paliar los daños, las medidas técnicas u organizativas previas, el grado de cooperación con la autoridad de control, o la forma en la que esta conoció la situación. Y es precisamente aquí donde el DPO cobra una gran trascendencia para el buen futuro económico y financiero de la organización, amén de para su buena imagen corporativa por su respeto a los derechos fundamentales de los ciudadanos que se relacionan con ella.
[35] Arts. 8, 11, 25 a 39, 42 y 43.
[36] Arts. 42 y 43.
[37] Art. 41.4.
[38] Arts. 5, 6, 7 y 8.
[39] Lesión que podrá ser habitual –arts. 12 a 22-.
[40] Arts. 44 a 49.

el responsable frente a los terceros de la falta de aplicación de las obligaciones que este establece. Debe tener medios y absoluta independencia, sin que pueda recibir instrucciones de otras esferas de la organización, siempre con directa relación con el más alto nivel jerárquico del tratamiento de los datos.

16.- El DPO exigirá inversiones y esfuerzos a las empresas, pero a su vez puede evitar o rebajar las graves y elevadas posibles sanciones impuestas a las mismas por las autoridades de control. Con toda esta configuración podrá ser una figura potencialmente conflictiva, en especial en Estados con poca o ninguna tradición en su existencia, pero creemos que es un actor esencial y de mucho futuro a partir del 28 de mayo de 2018 en la protección del Derecho fundamental a tratamiento de datos de los ciudadanos y con ello en la responsabilidad social corporativa de las empresas.

Resumen

La Unión Europea ha adaptado su antigua regulación de 1999 de la Directiva sobre protección de datos a los tiempos actuales a través del Reglamento (UE) 2016/679, de 27 de abril de 2016. Entre sus novedades introduce de forma generalizada en el Derecho europeo la figura del Delegado de protección de datos, de amplia raigambre en la UE y en algunos estados miembros, como Alemania. Las funciones del Delegado son muy importantes, y en especial su papel asesor y protector de las buenas prácticas de las empresas y de su responsabilidad frente a terceros. Su estatus y situación en la propia dinámica interna de la sociedad lo convierten en una figura con posibles futuros claroscuros, en especial en estados, como los del sur de Europa, que no tienen una asentada tradición en este tipo de figuras. En el otro plato de la balanza el Reglamento establece severas sanciones para las Instituciones y empresas que vulneren la norma, sanciones que las pueden llevar a situaciones límite, y que una buena actuación del DPO puede reducir. Todo ello motiva esta primera reflexión sobre cómo esta figura podrá influir en la protección del derecho fundamental a la protección de datos en la Unión.

Palabras clave

Derecho europeo, derecho a la intimidad, ciudadanía, seguridad, delegado de protección de datos.

Abstract

The European Union has adapted its former 1999 regulation of the Directive on Data Protection to current times through the Regulation (EU) 2016/679 of 27 April 2016. Among its changes, it extensively introduces in the European law the figure of the Data Protection Officer (DPO), of wide popularity nowadays in the EU and in some countries, as Germany. The functions of the Officer are very important, and especially his role as adviser and protector of the good practices of the companies and their responsibility towards third parties. His status and position in the internal dynamics of the company makes him an uncertain figure, especially in states such as those in Southern Europe, which do not have a settled tradition in this type of figures. At the other end of the scale, the Regulation imposes severe sanctions for institutions and companies that violate the rule, sanctions that can lead them to limit situations, and that can reduce a good action of the DPO. For all these reasons, we contribute an initial reflection on to what extent this figure of the Regulation on data protection could affect the protection of the fundamental right to the protection of personal data in the Union.

Key words

European law, right to privacy, citizenship, security, data protection officer.