Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

RESPONSABILIDAD SANCIONADORA DE LAS ADMINISTRACIONES PÚBLICAS EN MATERIA DE PRIVACIDAD: ESPECIALIDADES DEL ORDENAMIENTO JURÍDICO ESPAÑOL Y COMUNITARIO

SANCTIONING RESPONSIBILITY OF PUBLIC ADMINISTRATIONS IN MATTERS OF PRIVACY: SPECIALITIES OF THE SPANISH AND COMMUNITY LEGAL SYSTEM

Juan Francisco Rodríguez Ayuso
Profesor Ayudante Doctor de Derecho Administrativo
Universidad Internacional de La Rioja, UNIR (España)

Fecha de recepción: 11 de noviembre de 2020.

Fecha de aceptación: 20 de abril de 2021.

RESUMEN

El objetivo principal del presente estudio de investigación consiste en ofrecer un análisis sistemático de las novedades que trae consigo la entrada en vigor de la nueva normativa en materia de protección de datos personales en el ámbito de la responsabilidad propia, penal, civil y administrativa, de los responsables del tratamiento. Más concretamente, persigue exponer de manera más pormenorizada el ámbito concreto de responsabilidad en que pueden incurrir las Administraciones públicas y la naturaleza que esta responsabilidad presenta.

ABSTRACT

The main objective of this research study is to offer a systematic analysis of the new developments brought about by the entry into force of the new legislation on the protection of personal data in the field of the personal, criminal, civil and administrative liability of data controllers. More specifically, it seeks to explain in greater detail the specific area of responsibility in which the public administrations may incur and the nature of this responsibility.

PALABRAS CLAVE

RGPD, LOPDGDD, responsabilidad, Administraciones Públicas, datos personales.

KEYWORDS

GDPR, LOPDGDD, responsibility, Public Administrations, personal data.

ÍNDICE

SUMMARY

1. INTRODUCTION. 2. RESPONSIBILITY OF THE CONTROLLER. 2.1. Criminal liability. 2.2. Liability of a civil nature. 2.3. Liability of an administrative nature. 2.3.1. Uniform protection and mandatory compliance by Member States. 2.3.2. General regime (any factual or legal activity or lack of activity by the controller). 2.3.3. System of direct liability of the controller and/or processor. 2.3.4. System of subjective liability requiring the convergence of intent, fault or negligence, where fault in vigilance is considered to be included. 2.3.5. Integral repair of the damage produced by the processing operation. 2.3.6. Non-contractual liability in favor of the holders of the personal data 2.3.7. Joint and several liability. 2.3.8. Action for claim of liability for damage. 2.3.9. The system of sanctions. **3. INFRACTIONS BY GENERAL GOVERNMENTS. SPECIAL SANCTIONING REGIME. 4. WARNINGS AND CAUTIONS. 5. BIBLIOGRAPHY.**

1. INTRODUCCIÓN.

A lo largo de estas páginas analizaremos, en primer lugar, el amplio conjunto de obligaciones que, al amparo del principio de responsabilidad proactiva, tanto el Reglamento (UE) 2016/679 del Parlamento Europeo 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 (en adelante, Reglamento general de protección de datos o

RGPD)[1], como la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD)[2] establecen en torno a la figura del responsable del tratamiento. Este principio, que iremos perfilando, constituye la base y el fundamento de la obligatoria acreditación de cada actuación y de la observancia de una adecuada diligencia en el desarrollo de las operaciones de tratamiento sobre los datos personales del interesado en cuanto titular de los datos, así como el elemento fundamental para, bien no incurrir, bien mitigar la responsabilidad.

Como veremos, las consecuencias jurídicas que pueden desprenderse de la realización de operaciones de tratamiento de los datos personales son muy numerosas, si bien nos detendremos en aquellas que, específicamente, hacen nacer la responsabilidad del responsable del tratamiento (entendido como la persona, física o jurídica, de naturaleza pública o privada, que establece y determina los fines del tratamiento y los medios empleados para llevar a cabo aquellos), responsabilidad que puede ponerse de manifiesto en tres áreas muy diferentes: la penal, la civil y, en su caso, la administrativa. En la primera de ellas, se encuentran los delitos o los ilícitos de naturaleza penal; en la segunda, la obligación de indemnizar por los daños y perjuicios ocasionados, y, en tercer y último lugar, las infracciones de naturaleza administrativa.

2. RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO.

La responsabilidad del responsable del tratamiento, recogida en los artículos 24 RGPD y 28 LOPDGDD, puede manifestarse en tres ámbitos muy diferentes: el penal, el civil y el administrativo. A lo largo de las siguientes líneas analizaremos cada uno de ellos, si bien parece adecuado comenzar trasladando, de un modo literal, cuanto establecen sendos preceptos.

De acuerdo con el primero de ellos, el que proviene del ámbito comunitario:

«1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, 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. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento».

1 Diario Oficial de la Unión Europea (en adelante, DOUE) L 119/1, de 04 de mayo de 2016.

2 Boletín Oficial del Estado (en adelante, BOE), núm. 294, de 06 de diciembre de 2018.

Atendiendo, por su parte, a la normativa nacional, que completa y desarrolla los postulados del RGPD, se encuentra el artículo 28 LOPDGDD, intitulado Obligaciones generales del responsable y encargado del tratamiento, que establece cuanto sigue a continuación:

«1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación».

2.1. Responsabilidad de naturaleza penal.

Al hablar de la responsabilidad de tipo penal del responsable del tratamiento, estaremos hablando de aquellas acciones que, con anterioridad a la reforma del código penal efectuada en el año 2015, ya incluían conceptos que provenían de la normativa en materia de protección de datos personales y que, con la nueva regulación, han quedado desvirtuadas, en especial si tenemos en cuenta su denominación, ya que, entre otros, no se alude al término responsable del fichero, sino de responsable el tratamiento.

En este sentido, conviene destacar el artículo 197 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en adelante, Código Penal)[3], que impone condena de prisión de uno a cuatro años y multa de doce a veinticuatro meses para todos aquellos que, de una manera u otra y sin el consentimiento de las personas físicas titulares de los datos, descubran secretos o vulneran la intimidad de otro. Las acciones previstas en el apartado primero de dicho precepto son múltiples y algunas de las mismas pueden conllevar, con carácter previo, el acceso indebido a datos personales como vía para entrar, por ejemplo, en la cuenta de correo electrónico de la víctima.

Con el fin de impedir que, por ausencia de una adecuada regulación, no fueran castigadas este tipo de conductas, el apartado segundo de este mismo precepto dispone idénticas penas para todos aquellos que realicen acciones de apoderamiento, utilización o modificación, contra un tercero, de datos personales reservados o de cualquier otro dato personal o familiar que se encuentre incorporado a un fichero o soporte de naturaleza informática, electrónica o telemática, o en cualquier otro tipo de archivo o registro, ya sea público o privado. Junto a lo anterior, por si no fuera suficientemente contundente la tipificación expuesta, se señala que se seguirán imponiendo idénticas sanciones a aquellos que, sin contar con autorización de ningún tipo, accedan de cualquier forma a los ficheros y soportes anteriores, así como a aquellos que procedan a alterarlos o utilizarlos en perjuicio del titular de los datos personales o de un tercero.

Conviene subrayar que, para ser responsable penal, resulta imprescindible la concurrencia de dolo (Ventura Püschel, 2018), ya que se exige la intención de dañar la privacidad, apropiarse de información, emplearla o modificarla en perjuicio de terceros, es decir, actuaciones que, de un modo claro, traigan aparejado un ánimo o intención dañosa. Idéntica conclusión cabe extraer de otro tipo de actuaciones que pueden ser realizadas de manera imprudente, como apropiarse del correo o acceder por error o sin advertencia a los ficheros y soportes que incluyan información de terceros, ya que, en atención al contexto en el que se encuentran, es imprescindible una comprobación de que este acceso se ha producido con la intención de aprovecharse de dicha información para provocar un perjuicio al propietario de los datos personales o a un tercero o, como mínimo, obtener un beneficio de esta información. Así las cosas, el acceso accidental a la información por error o, como

3 BOE núm. 281, de 24 de noviembre de 1995.

suele suceder de manera más habitual, porque el responsable del tratamiento no ha implementado medidas de seguridad adecuadas, no determinará el nacimiento de responsabilidad de naturaleza penal, con independencia de que pueda concurrir responsabilidad de naturaleza administrativa por parte del responsable del tratamiento.

Por su parte, el apartado tercero del artículo 197 del Código Penal reitera lo ya establecido con anterioridad, incrementando la pena de dos a cinco años de prisión si se realiza algún tipo de difusión, revelación o cesión a terceros de los datos personales o hechos descubiertos o si las imágenes han sido obtenidas por medio de alguna de estas acciones. Las acciones ilícitas descritas lo son cuando desembocan tradicionalmente en determinados daños para aquellos que han visto vulnerada su privacidad, así como en lucro para el infractor. Así, se castigan incluso, si bien con una pena inferior (de uno a tres años de prisión y multa de doce a veinticuatro meses), todos aquellos que, sin haber tomado parte en su descubrimiento, realizan su difusión siendo conscientes de su origen ilícito.

Los delitos aludidos pueden ser cometidos por aquellos sujetos que desarrollan actividades de ciberdelincuencia y por responsables y encargados del tratamiento. En este caso, el apartado cuarto del artículo 197 del Código Penal incrementa la pena de prisión hasta cinco años en el supuesto de que, quien realice las conductas contempladas en los apartados primero y segundo de este precepto, sea un responsable o un encargado del tratamiento. En el caso de que los datos personales hayan sido objeto de difusión, cesión o revelación a terceros, las penas se impondrán en su mitad superior. De igual modo, y aun cuando no se haya producido cesión o difusión de los datos personales, idénticas penas serán impuestas si estamos en presencia de categorías especiales de datos personales (artículo 9 RGPD) que difundan aspectos relacionados con la ideología, religión, creencias, salud, origen racial o vida sexual, en el caso de que el afectado sea un niño o un sujeto con discapacidad o en el supuesto de que, sin afectar a este tipo de datos personales especialmente protegidos, haya intervenido con ánimo de lucro; si, amén de concurrir este ánimo de lucro, se lleva a cabo el tratamiento de categorías especiales de datos personales o de datos personales relativos a niños o personas con discapacidad, la pena se vería incrementada de modo significativo, habiéndose de imponer sanciones de entre cinco a siete años y multas de doce a veinticuatro meses en su mitad superior.

Por último, idénticos hechos podrán ser realizados por autoridades y demás personas que trabajen al servicio de las Administraciones Públicas. En este supuesto, las condenas anteriormente indicadas se impondrán, también, en su mitad superior, tal y como establece el artículo 198 del Código Penal.

A lo anterior habría que sumar, dado su carácter novedoso y las consecuencias jurídicas que trae aparejadas, el artículo 197 bis del Código Penal, que amplía la protección frente a aquellos que, por cualquier medio o procedimiento, vulneran las medidas de seguridad contempladas para impedirlo [al amparo de los artículos 5.1.f) y 32, ambos del RGP]) y, sin contar con la debida autorización, facilitan a otros el acceso al conjunto o a una parte de un sistema de información, imponiéndoles una pena de prisión de entre seis meses a dos años. Dicho artículo, que fue incorporado en el año 1995 a la norma, ha sido objeto de numerosas críticas por parte de la doctrina (Sierra

López, 2018), además de por el hecho de que cabe la posibilidad de que el autor no entre en prisión por no exceder la pena de dos años, porque considera también el acceso a un sistema de información previamente contemplado con una mayor pena en el artículo 197 del Código Penal, pudiendo ocasionar evidentes disfunciones que escapan del ámbito de este estudio.

Por su parte, el artículo 197 ter del Código Penal alude al hecho de producir, adquirir o distribuir a terceros programas informáticos, previstos para la comisión de los delitos referidos; una contraseña de ordenador; un código de acceso, o datos similares que hagan posible el acceso a todo o parte de un sistema de información. En este caso, se impondrá a la empresa una pena de multa de entre seis meses a dos años y, teniendo en consideración las reglas contempladas en el artículo 66 bis del Código Penal, los jueces y tribunales podrán, de igual modo, imponer aquellas multas contempladas en las letras b) a g) del apartado séptimo del artículo 33 del Código Penal, entre las que se incluyen la disolución de la persona jurídica, la suspensión de sus actividades por un plazo que no podrá ser superior a cinco años o el cierre de sus locales.

Para concluir, el artículo 197 quinquies del Código Penal es especialmente relevante para las empresas de cloud o que prestan sus servicios en la nube (Carrasco Sayalero, 2019). Entre los motivos se encuentra que, dada la propia dinámica de las actividades desarrolladas y el complejo trabajo que pueden conllevar, cabe la posibilidad de que se vean obligadas a no suprimir los datos personales del interesado una vez finalizada la prestación del servicio, así como a acceder a aquellos datos personales almacenados pese a que estos estén cifrados. En este sentido, para este tipo de empresas resulta especialmente adecuada la figura del delegado de protección de datos (artículos 37 a 39 RGPD y 34 a 37 LOPDGDD), así como la implementación de protocolos de compliance o cumplimiento legal, especialmente aptos para evitar, de manera inmediata y desde el inicio, la apertura de un procedimiento de naturaleza legal, a menudo engorroso para una empresa.

2.2. Responsabilidad de naturaleza civil.

En cuanto a la responsabilidad civil, podemos decir que esta se encuentra inmanentemente relacionada con las responsabilidades de naturaleza penal y administrativa (García-Panasco Morales, 2019). La razón estriba en que, aun cuando la responsabilidad civil goza de autonomía propia y, por ende, puede nacer más allá de que no se haya producido ninguna infracción que determine el surgimiento de responsabilidad penal o administrativa, en aquellos casos en que existe una infracción, queda acreditada la exigencia de dolo o culpa, requisito imprescindible para el surgimiento de la obligación de indemnización en vía civil por los daños o perjuicios ocasionados al interesado. Así las cosas, el considerando 146 RGPD dispone la obligación general del responsable o del encargado del tratamiento de indemnizar cualquier daño o perjuicio que pueda padecer una persona como resultado de la realización de una operación de tratamiento realizada en infracción de la nueva normativa sobre esta materia. En consecuencia, podemos afirmar que existen dos ámbitos de responsabilidad: un primer ámbito, que surge del incumplimiento de la nueva normativa en materia de protección de datos personales y que determina la

obligación de indemnización el daño; un segundo ámbito, que consiste en la facultad de demostrar la inexistencia de responsabilidad en la comisión de daños y perjuicios y que va unido a la adopción de medidas técnicas y organizativas al amparo de los artículos 24 RGPD y 28 LOPDGDD.

Por su parte, el considerando 74 RGPD sostiene que ha de quedar establecida la responsabilidad del responsable del tratamiento derivada de cualquier tratamiento de datos personales que haya sido realizado por él o por cuenta de él. Esta afirmación, aunque parece desplazarnos al supuesto típico de responsabilidad contemplada en el artículo 1902 del Código Civil[4], no es así, ya que dicho considerando sigue estableciendo la obligación del responsable del tratamiento de, no sólo implementar medidas solventes y eficaces, sino acreditar la adecuación de las actividades de tratamiento a la normativa aplicable (Marcos Ayjón, 2017). La diferencia parece obvia, ya que se invierte la carga de la prueba, de modo que quien exige el daño no tiene la obligación de acreditar la culpa o negligencia de quien sostiene que lo ha causado, sino que será este último quien deberá demostrar que su conducta se realizó diligentemente; más incluso, aun en el supuesto de que pudiera demostrar que actuó diligentemente, cabe la posibilidad de que tenga que proceder a la indemnización por los daños y perjuicios ocasionados, habida cuenta de lo establecido en los tres primeros apartados del artículo 82 RGPD, que parecen imponerlo. Ello podría desembocar en determinadas afectaciones a la esfera de responsabilidad de las Administraciones Públicas.

En cualquier caso, el deber de adopción de medidas ha de ser proporcional al riesgo que conlleva la realización de actividades de tratamiento y, en aquellos supuestos contemplados en el considerando 84 RGPD, cuando la evaluación de impacto ponga de manifiesto que las actividades de tratamiento comportan un riesgo elevado que el responsable del tratamiento no es capaz de reducir con la adopción de medidas eficaces en términos de tecnología disponible, con anterioridad al inicio de dicha operación de tratamiento, será imprescindible consultar a la autoridad de control (artículos 35 y 36 RGPD). Habida cuenta de que, en estos supuestos, no se suprime el riesgo, pese a la implementación de medidas de carácter preventivo, se asume la probabilidad de generación de daños. Será imprescindible el acierto, ya sea en la cuantificación del posible daño, ya sea en la imposición de medidas que tiendan a su indemnización, con el fin de impedir que, debido a la previa decisión administrativa de autorizar la realización del tratamiento, puedan derivarse acciones de responsabilidad patrimonial.

Por lo demás, en aquellos casos en los que el responsable del tratamiento sea una Administración Pública, la responsabilidad será objetiva, ya que así lo establece el artículo 106.2 de la Constitución Española[5]. Así las cosas, la acomodación de la conducta a la nueva normativa sobre protección de datos no evitará la obligación de indemnización, ya que es suficiente la demostración de que la causa del daño se deba al funcionamiento o a la actuación de la Administración, que el daño es valorable económicamente y que el interesado no tiene la obligación jurídica de soportarlo,

4 Gaceta de Madrid núm. 206, de 25 de julio de 1889.

5 BOE núm. 311, de 29 de diciembre de 1978.

para que surja, por exigencia constitucional, la obligación de indemnización de los daños ocasionados. En este sentido, el régimen de responsabilidad de las Administraciones Públicas, a diferencia del contemplado en el artículo 1902 del Código Civil, será objetivo, de modo que no es imprescindible la demostración de la existencia de dolo o negligencia en la actuación que motiva el daño.

2.3. Responsabilidad de naturaleza administrativa.

Una tercera y última modalidad de responsabilidad que puede recaer sobre el responsable del tratamiento es aquella de tipo administrativo. Hasta ahora, esta responsabilidad se encontraba recogida en los artículos 43 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD)[6], preceptos estos que, indudablemente, se han visto afectados como consecuencia de la aplicación del Reglamento general de protección de datos y de la nueva LOPDGDD. El motivo es, de un lado, que el considerando 150 RGPD alude a la necesidad de llevar a cabo una necesaria armonización, efectuada por el artículo 83 RGPD, estableciendo las infracciones y los límites máximos y criterios de la sanciones; de otro, que el considerando 152 del mismo Reglamento posibilita que, en aquellos supuestos en los que la nueva normativa no lleve a cabo la armonización de las sanciones administrativas, los países comunitarios deberán implementar un sistema que imponga sanciones efectivas, proporcionadas y disuasorias (este régimen sancionador quedará fijado, en nuestro ordenamiento jurídico interno, en los artículos 70 a 78 LOPDGDD).

Con carácter previo, parece adecuado comenzar transcribiendo, de un modo literal, el contenido del artículo 82 RGPD, como trámite necesario de cara a la presentación de los rasgos definitorios del derecho a indemnización y del sistema de responsabilidad en el ámbito de la protección de los datos. En consecuencia, y de acuerdo con el citado precepto:

«1. 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.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá 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.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

[6] BOE núm. 298, de 14 de diciembre de 1999.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2».

Así las cosas, entre los principios del sistema de responsabilidad y las características del derecho a indemnización que configuran el artículo 82 de la nueva normativa comunitaria en materia de protección de datos personales, podemos encontrar los principios que a continuación se relacionan:

2.3.1. Protección homogénea y de cumplimiento obligatorio para los Estados miembros.

La regulación actual sobre protección de datos persigue, como objetivo fundamental, garantizar un nivel uniforme y superior de protección de las personas físicas y suprimir los obstáculos a la libre circulación de datos dentro del territorio comunitario, consolidando un nivel adecuado de protección de los derechos y libertades de los interesados en lo que atañe al tratamiento de sus datos personales al ser este equivalente en todos los Estados miembros.

El legislador admite que, si bien las finalidades perseguidas por los principios de la 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, DPDP)[7] continúan siendo válidos, la protección de datos dentro del territorio de la Unión Europea ha sido aplicada fragmentariamente, generando una suerte de inseguridad jurídica, además de la apreciación por los ciudadanos de la existencia de riesgos relevantes en lo que concierne al tratamiento de sus datos personales.

Es por ello por lo que el Reglamento general de protección de datos proporciona un tratamiento unitario y uniforme del régimen jurídico del derecho fundamental a la protección de los datos personales de las personas físicas, dentro del cual, como medida para resarcir el daño ocasionado, se incorpora la regulación de la

[7] Diario Oficial de las Comunidades Europeas (en adelante, DOCE) L 281/31, de 23 de noviembre de 1995.

responsabilidad del responsable y/o del encargado del tratamiento de los datos personales del interesado.

Al contrario del artículo 23 DPDP que incorporaba un mandato a los Estados miembros para que disciplinasen el Derecho indemnizatorio en favor de aquellos interesados que hubieran padecido un tratamiento ilícito de sus datos personales, la regulación incorporada por el artículo 82 RGPD en relación con este derecho de los interesados goza de carácter uniforme y es de obligada satisfacción por todos los países comunitarios, con las preceptivas adecuaciones a los sistemas de responsabilidad civil o patrimonial de cada uno de estos países (Martínez Martínez, 2019).

2.3.2. Régimen general (toda actividad fáctica o jurídica o falta de actividad por parte del responsable del tratamiento)

El artículo 82.2 RGPD dispone la responsabilidad del responsable del tratamiento que participe en la operación de tratamiento y que habrá de responder de los daños y perjuicios ocasionados en el supuesto de que esta operación no satisfaga lo establecido por la nueva normativa en materia de protección de datos personales; en otras palabras, este apartado configura la responsabilidad del responsable del tratamiento en aquellos casos de participación en una operación y de no cumplimiento, ya sea por una actuación activa o pasiva, de lo establecido en la regulación vigente sobre protección de los datos personales (Busto Lago, 2020).

Aun cuando el artículo 82 RGPD disciplina la responsabilidad del encargado del tratamiento de un modo más limitado, pues tan sólo responderá de los daños y perjuicios ocasionados por el tratamiento en aquellos casos en que no haya satisfecho las obligaciones impuestas por la normativa o haya intervenido al margen o contrariamente a las instrucciones legales impuestas por el responsable del tratamiento, la realidad es que tales deberes o instrucciones podrán ser fácticas, jurídicas, activas o pasivas, de modo que no desvirtúa las regulación del encargado del tratamiento el principio del régimen general que establece el Reglamento general de protección de datos.

Por lo que respecta al hecho de que un tratamiento de los datos no satisfaga lo establecido en la nueva normativa en materia protección de datos personales, el Reglamento general de protección de datos aclara que ello abarcará aquellos tratamientos que infrinjan, además de las disposiciones de este texto, los actos delegados y de ejecución que se implementen de acuerdo con la normativa comunitaria en materia de protección de datos, así como las normas de los Estados miembros que sean objeto de adopción desarrollando o cumpliendo el Reglamento general de protección de datos. En consecuencia, la acción de reclamación de responsabilidad nace en aquellos casos en que se incumpla con lo establecido en dicho Reglamento, en los actos delegados y ejecutivos implementados al amparo del mismo y en las normas internas sobre esta cuestión, como sucede, en nuestro país y con carácter fundamental, con la LOPDGDD.

2.3.3. Sistema de responsabilidad directa del responsable y/o del encargado del tratamiento

El RGPD establece que será el responsable o el encargado del tratamiento ilícito quienes habrán de responder de los daños ocasionados por la operación de tratamiento en aquellos supuestos en que el responsable el tratamiento no cumpla lo establecido en la nueva normativa en materia protección de datos personales o el encargado del tratamiento no satisfaga los deberes impuestos de manera concreta por la precitada normativa o por las instrucciones marcadas por el responsable del tratamiento.

El Reglamento general de protección de datos configura, así, la responsabilidad directa del responsable del tratamiento ilícito que origine daños al titular de los datos personales, ya sea porque el tratamiento fue realizado por el mismo directamente, ya sea por medio de un tercero siguiendo sus instrucciones (encargado del tratamiento), al amparo de cuanto establecen los artículos 28 RGPD y 28 LOPDGDD. En este último caso, el encargado del tratamiento cuenta con una responsabilidad ciertamente más restringida, habida cuenta de que únicamente va a responder de los daños ocasionados en aquellos casos en que no cumpla las obligaciones marcadas por la normativa, que son más reducidas que las que recaen sobre el responsable del tratamiento, si bien también responderá cuando no obedezca las instrucciones marcadas por este.

Esta limitación de la responsabilidad que recae en el encargado del tratamiento tiene una razón de ser, pues no debemos olvidar que el encargado del tratamiento ha de intervenir siempre bajo el mandato del responsable del tratamiento (Ordóñez Pineda, 2019).

2.3.4. Sistema de responsabilidad subjetiva que requiere de la convergencia de dolo, culpa o negligencia, donde se considera incluida la conocida como culpa *in vigilando*

La nueva normativa en materia de protección de datos se decanta por el principio de responsabilidad subjetiva, de aplicación en todos los Estados miembros de la Unión Europea, incluyendo aquí los daños ocasionados por la Administración pública. En este sentido, el sistema configurado por nuestro país acoge el principio de responsabilidad subjetiva tanto en Derecho civil como en Derecho penal, si bien no procede de igual forma en Derecho administrativo, en el que se incorpora una palpable distinción en relación con los Estados de nuestro alrededor, toda vez que, en España, la Administración Pública habrá de responder por los daños ocasionados con su actuación, activa o pasiva, por medio de actos jurídicos o de actuaciones fácticas, más allá de que sus agentes intervengan con dolo, culpa o negligencia; de este modo, se establece la responsabilidad objetiva derivada del funcionamiento normal o anormal de los servicios públicos (Romeo Ruiz, 2020).

Pues bien, la regulación interpuesta por la nueva regulación sobre protección de datos en cuanto al Derecho indemnizatorio se asemeja más a la responsabilidad subjetiva, por dolo, culpa o negligencia que, como se ha puesto de manifiesto, preside los sistemas jurídicos internos de nuestro alrededor y que, por ende, resulta de

aplicación para determinar la responsabilidad extracontractual de las instituciones y organismos comunitarios, de conformidad con lo establecido por el artículo 340 del Tratado de Funcionamiento de la Unión Europea[8].

De este modo, el artículo 82.3 RGPD exime de responsabilidad por los daños ocasionados en las operaciones de tratamiento de datos personales al responsable y/o al encargado del tratamiento en aquellos casos en que puedan demostrar que no son, de ninguna manera, responsables del hecho que haya originado tales daños o perjuicios.

No obstante, habida cuenta de la conformación que presenta el sistema de responsabilidad patrimonial de la Administración pública en nuestro país, basado en un sistema de responsabilidad objetiva en aquellos casos en que el responsable o el encargado del tratamiento sea personal de la Administración española, el titular de los datos personales afectado por el tratamiento ilícito tendrá la posibilidad, siempre que concurran las exigencias marcadas por los artículos 32 a 34 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP)[9], de implementar la acción de reclamación de responsabilidad patrimonial contra tal Administración, aun cuando no exista ni concurra dolo, culpa o negligencia en el mismo. Sin embargo, la Administración que sea responsable del daño ocasionado no tendrá la posibilidad de repetición de la indemnización satisfecha frente a su personal si este no incurre en dolo, culpa o negligencia, pues así lo establece el apartado segundo del artículo 36 LRJSP.

2.3.5. Reparación integral de los daños producidos con la operación de tratamiento

De conformidad con el artículo 82.1 RGPD, serán objeto de indemnización aquellos daños y perjuicios de naturaleza material o inmaterial, de modo que se proporciona una reparación total que abarca tanto los daños físicos y patrimoniales, como también los morales.

En los considerandos de la nueva normativa comunitaria en materia de protección de datos personales se establece que el concepto de daños y perjuicios ha de concebirse en un sentido amplio, de acuerdo con la jurisprudencia del Tribunal de Justicia de la Unión Europea, de tal forma que se hagan respetar de manera plena los fines perseguidos por el Reglamento general de protección de datos. Con ello, se pone de manifiesto la necesidad de respetar el objetivo último de proteger una reparación integral de los daños ocasionados como consecuencia de las operaciones de tratamiento realizadas.

Como es obvio, y aun cuando el artículo 82 RGPD no lo diga expresamente, el daño tendrá que ser efectivo, real, evaluable de manera económica e individualizable con relación a un individuo o grupo de individuos, como también ocurre con el Derecho nacional. Algunas veces, cuando el daño sea hipotético o no se haya

[8] DOUE C 83/47, de 30 de marzo de 2010.

[9] BOE núm. 236, de 02 de octubre de 2015.

producido de manera real, habida cuenta del escaso intervalo en el que los datos fueron objeto de exposición, los tribunales se han opuesto a esta indemnización, bajo la premisa de que la reparación de la lesión del derecho fundamental a la protección de los datos personales se ha producido con la sentencia declarativa.

Al contrario de lo que ocurre con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[10], el artículo 82 RGPD no disciplina una presunción de existencia de perjuicio en aquellos casos en que sea acreditada la infracción de la normativa contenida en el propio Reglamento. Resultado de lo anterior, será necesaria la prueba de la concurrencia del daño ocasionado y, de igual modo, la relación de causalidad existente entre la actuación u omisión del responsable del tratamiento y el daño efectivamente ocasionado.

2.3.6. Responsabilidad extracontractual en favor de los titulares de los datos personales

La regulación proporcionada por la nueva normativa en materia de protección de datos conlleva una garantía para los interesados cuyos datos personales se someten a operaciones de tratamiento, aun cuando no intervenga un contrato entre el titular de los datos (interesado) y el responsable o el encargado del tratamiento.

Así, se instruye, de manera novedosa, la obligatoria indemnización que habrá de proporcionarse como consecuencia de los daños ocasionados por tratamientos que no sean adecuados a lo establecido en la normativa vigente sobre la materia. Estamos en presencia, por ende, de la responsabilidad por daños, con finalidad resarcitoria, que no se origina por un incumplimiento contractual y que, en consecuencia, no persigue un resarcimiento de este incumplimiento.

2.3.7. Responsabilidad solidaria

El artículo 82 RGPD, en sus apartados cuarto y quinto, aborda de manera específica la regulación de la responsabilidad solidaria del responsable y/o del encargado del tratamiento.

En concreto, el artículo 82.4 de la nueva normativa comunitaria dispone que cada responsable o encargado del tratamiento tendrá la consideración de responsable de la totalidad de los daños y perjuicios (Rodríguez Ayuso, 2020), con el objetivo de garantizar una indemnización efectiva del titular de los datos personales, de modo que proporciona una regulación de la responsabilidad solidaria, caracterizada, precisamente, por esa opción que tiene el interesado que se vea perjudicado de acudir a un responsable o al encargado de tratamiento para exigirle la satisfacción total de la indemnización que proceda.

A su vez, como fácilmente puede deducirse dentro de la responsabilidad solidaria a que prestamos atención, el artículo 82.5 RGPD establece que aquel que

[10] BOE núm. 115, de 14 de mayo de 1982.

llevó a cabo la satisfacción integral de la indemnización tendrá derecho de repetición contra el resto de los sujetos responsables por la parte que a cada uno de ellos le corresponda satisfacer. El objetivo perseguido consiste, por tanto, en hacer posible que el interesado que ha padecido un daño derivado de un tratamiento ilícito de sus datos personales no se vea obligado a tener que acudir a cada uno de los responsables o encargados del tratamiento una vez obtenida una resolución judicial favorable que le reconoce un derecho de indemnización con el fin de conseguir la satisfacción integral de la indemnización así reconocida.

Al decantarse por este sistema de responsabilidad solidaria, la regulación en vigor sobre protección de datos pone de manifiesto su objetivo de garantizar una indemnización efectiva en favor del titular de los datos personales, tal y como se desprende del artículo 82.4 RGPD.

2.3.8. Acción de reclamación de responsabilidad por daños

El artículo 82.6 RGPD dispone el lugar al que debe dirigirse el titular de los datos personales afectado para poder interponer su reclamación de responsabilidad patrimonial, aludiendo a los tribunales competentes de los Estados miembros y remitiéndose a lo establecido en el apartado segundo del artículo 79 del mismo Reglamento.

Este último apartado de la nueva normativa comunitaria en materia protección de datos personales establece que las acciones frente al responsable y/o encargado del tratamiento habrán de interponerse, en primer lugar, ante los tribunales nacionales competentes en los que este responsable o encargado el tratamiento tengan su establecimiento. No obstante, seguidamente, establece que, de manera alternativa, estas acciones podrán ser ejercitadas ante los tribunales del Estado miembro donde el titular de los datos tenga su residencia habitual, siempre que el responsable o el encargado del tratamiento no sea una autoridad pública de un Estado miembro que intervenga en ejercicio de sus poderes públicos.

La cuestión que se plantea al analizar este apartado radica en determinar si se refiere a los tribunales de los Estados miembros en los que el responsable o el encargado del tratamiento tengan su establecimiento o a los tribunales en los que tenga su domicilio quien interpone la acción de reclamación de responsabilidad.

Nuevamente, los considerandos del Reglamento general de protección de datos nos permiten interpretar, de un modo más claro, los apartados sexto y segundo de los artículos 82 y 79, respectivamente. Así pues, el legislador comunitario establece que quien interpone la reclamación debe tener la posibilidad de ejercitar las acciones frente al responsable o al encargado del tratamiento ante los tribunales de los Estados miembros en los que estos tengan su establecimiento o, si así lo prefiere, ante los tribunales de los países comunitarios en los que él mismo reclamante tenga su domicilio.

No obstante, como hemos visto, esta posibilidad del reclamante tan sólo se vería suprimida en el caso de que el responsable o el encargado del tratamiento sea una autoridad pública de un Estado miembro que intervenga en ejercicio de sus poderes públicos. En este caso, el reclamante de indemnización tendrá que interponer

su acción frente a los tribunales competentes del Estado miembro de la autoridad pública, únicos competentes para poder conocer la responsabilidad por daños derivados del tratamiento ilícito de los datos personales del interesado en este concreto supuesto; ello puede interpretarse, de forma contraria, en el sentido de que, en aquellos casos en que la Administración no intervenga en ejercicio de sus poderes públicos, el titular de los datos personales afectado por el tratamiento ilícito tendrá la posibilidad de interponer la acción de responsabilidad en el Estado miembro en el que tuviese su domicilio.

Aun cuando la nueva normativa en materia de protección de datos introduce el concepto amplio de establecimiento del responsable y del encargado del tratamiento que ha elaborado a lo largo del tiempo la jurisprudencia del Tribunal de Justicia de la Unión Europea, también es cierto que el legislador pone de manifiesto que el concepto de establecimiento habrá de determinarse atendiendo a las circunstancias de cada supuesto específico (Rotondo Tornaría, 2019). En consecuencia, con el objetivo de posibilitar la máxima que orienta la regulación del derecho a indemnización por los daños originados por un tratamiento ilícito de los datos personales, cual es la de proteger una indemnización efectiva de los mismos, esta nueva regulación opta por otorgar al interesado la posibilidad de interponer su acción de reclamación, no sólo ante los tribunales de los Estados miembros en los que el responsable o encargado del tratamiento tienen su establecimiento, sino, además, posibilitar que la acción de reclamación se interponga ante los tribunales competentes del país comunitario donde el mismo interesado tenga su domicilio.

Lo anterior supone, parece evidente, un avance importante en la tutela del derecho fundamental a la protección de los datos personales, que suprime el impedimento que comportaba, para la efectividad del derecho de indemnización, la obligación de tener que interponer la reclamación ante otro Estado miembro diferente de aquel en el que el titular de los datos personales afectado tuviera su domicilio, habida cuenta de que el responsable o el encargado del tratamiento tenían allí su establecimiento.

2.3.9. El régimen sancionador

El régimen sancionador contemplado en los artículos 83 y 84 RGPD y en los artículos 70 a 78 LOPDGDD (Título IX) incorpora relevantes novedades en relación con lo contemplado en la normativa comunitaria y en la legislación interna española precedentes. En este sentido, podemos advertir que estamos en presencia de una regulación abundante que suscita cuestiones relevantes en determinados aspectos.

De acuerdo con lo establecido en el considerando 11 RGPD, una garantía de los datos personales en el ámbito comunitario impone, además de otras cuestiones, que las infracciones de los deberes contemplados sean castigadas con sanciones equivalentes, ya sean de naturaleza económica o no. Así las cosas, se persigue que la vulneración del derecho fundamental a la protección de datos no quede indemne en ningún punto del territorio de la Unión Europea.

Esto constituye, específicamente, uno de los más importantes fines que se busca con la nueva normativa en materia de protección de datos personales: lograr una armonización que imposibilite la concurrencia de regulaciones diversas. Por ello, una de las más feroces críticas vertidas sobre la regulación anterior aludía a la desmesurada libertad atribuida a los Estados miembros a la hora de configurar su correspondiente régimen sancionador, de modo que el tratamiento de las infracciones y sanciones podía verse alterado sustancialmente de un país comunitario a otro.

En relación con esta cuestión, se han pronunciado los considerandos 148 y 150 RGPD, al establecer que toda infracción habrá de verse castigada con sanciones, incluidas multas de naturaleza administrativa, con independencia de que sean atendidas las circunstancias específicas de cada supuesto. Lo que se persigue, en definitiva, es que todas las autoridades de control tengan la facultad de interponer multas administrativas derivadas de la realización o comisión de infracciones, de modo que no imperen los conocidos como "paraísos de datos" dentro del territorio comunitario que, en cierto modo, dificulten la libre circulación de los datos, obstruyan el ejercicio de las actividades económicas y falseen la competencia, imposibilitando que las autoridades de control satisfagan las tareas que les son atribuidas por el Derecho comunitario.

Sin embargo, la nueva normativa comunitaria no completa toda la disciplina del régimen sancionador, ya que, en determinados aspectos, deja margen, en mayor o menor medida, a los Estados miembros para que completen esta cuestión con su propia normativa nacional interna. Es entonces cuando aparecen los artículos 70 a 78 LOPDGDD, el primero de los cuales establece que estarán sujetos al régimen sancionador establecido en el RGPD y en la LOPDGDD:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

En cambio, no será de aplicación al delegado de protección de datos el régimen sancionador establecido en el Título IX LOPDGDD.

3. INFRACCIONES POR PARTE DE LAS ADMINISTRACIONES PÚBLICAS. RÉGIMEN SANCIONADOR ESPECIAL.

La nueva normativa en materia de protección de datos, como sucede también con la ya derogada, establecen que podrá ser responsable o encargado del tratamiento una persona física o jurídica, autoridad pública, servicio u otro organismo. Así las cosas, las Administraciones públicas también se verán sometidas a los deberes impuestos por la norma y, por tanto, podrán llegar a cometer infracciones, de conformidad con lo establecido en el artículo 83 RGPD (Romeo Ruiz, 2020). Otra cosa diferente es que, como consecuencia de que se cometa una determinada infracción,

estas Administraciones públicas no se vean sujetas al régimen sancionador establecido para los sujetos privados y, por ende, no se les imponga la correspondiente multa administrativa, bastando, simplemente, con una declaración de infracción.

De acuerdo con lo establecido en el artículo 83.7 RGPD, se atribuye a los Estados miembros cierto margen para establecer normas en relación a si es posible, y en qué medida, establecer multas administrativas a las autoridades y organismos públicos. Así las cosas, la normativa nacional interna podrá pronunciarse en torno al régimen jurídico relativo a la declaración de infracción que puede ser impuesta a las Administraciones públicas, en sustitución, en su caso, de las multas administrativas.

En este sentido, aparece el artículo 77 LOPDGDD, que regula el régimen aplicable a determinadas categorías de responsables o encargados del tratamiento, estableciendo que dicho régimen será de aplicación a los tratamientos de los que sean responsables o encargados del tratamiento:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las Comunidades Autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de Derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

En estos supuestos, cuando los responsables o encargados del tratamiento enumerados cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 LOPDGDD, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá, asimismo, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesados, en su caso (artículo 77.2 LOPDGDD).

Pese a lo anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En

este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación. Asimismo, cuando las infracciones sean imputables a autoridades y directivos y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el BOE o Boletín autonómico que corresponda (artículo 77.3 LOPDGDD).

En este sentido, se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan y se comunicará al Defensor del Pueblo o, en su caso, a las instituciones análogas de las Comunidades Autónomas las actuaciones realizadas y las resoluciones dictadas (artículo 77, apartados 4 y 5, LOPDGDD).

Por último, cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web, con la debida separación, las resoluciones referidas a las entidades antes enumeradas, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción. Por su parte, cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica (artículo 77.6 LOPDGDD).

4. APERCIBIMIENTOS Y ADVERTENCIAS

Para concluir, también genera interés el contenido del artículo 58 RGPD, que analiza todo lo relativo a los apercibimientos y a las advertencias. Al respecto, este artículo atribuye facultades a las autoridades de control para poder establecer sanciones por medio de advertencias a cualquier responsable o encargado del tratamiento cuando las operaciones puedan llegar a suponer una infracción de lo establecido en la normativa en materia de protección de datos.

Estas medidas de apercibimiento y advertencia podrán imponerse al responsable o al encargado del tratamiento de manera complementaria o sustitutiva a las multas de naturaleza administrativa. En principio, si una multa administrativa es impuesta con carácter sustitutivo, no suscita problemática alguna, pero, si se hace de modo complementario, sí puede llegar a significar un supuesto de doble imposición de sanción ante una misma conducta, incurriendo en aquello que prohíbe el principio de non bis in idem, ya que, tanto las multas administrativas como las medidas ahora analizadas tienen la calificación de sanciones por la nueva normativa en materia protección de datos personales.

La distinción fundamental entre las advertencias y los apercibimientos reside en que, mientras que en las advertencias la infracción puede haberse producido, para los apercibimientos la infracción ya ha debido producirse de manera fehaciente.

La regulación de los apercibimientos no supone problemática alguna, toda vez que ya estaban contemplados en la normativa precedente, si bien no tenía la consideración de verdadera sanción. No obstante, las advertencias sí que pueden suponer una mayor problemática, ya que no llega a concebirse suficientemente el hecho de que puedan imponerse medidas sancionadoras derivadas de operaciones de

tratamiento que puedan suponer una infracción de lo establecido en la normativa sobre protección de datos; en otras palabras, o se produce la conducta en que consiste la infracción, o no se produce, algo que deberá resolverse por medio de un procedimiento sancionador que cuente con garantías suficientes y por medio de pruebas que permitan desvirtuar el principio de presunción de inocencia, tal y como establece el artículo 83.8 RGPD.

5. BIBLIOGRAFÍA.

BUSTO LAGO, J. M., «Protección de datos personales y responsabilidad civil», en Herrador Guardia, M. J. (Coord.), Derecho de daños, 2020, 443-512.

CARRASCO SAYALERO, I., «Cloud Computing», en LÓPEZ CALVO, J. (Coord.), La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD, 2019, 943-959.

GARCÍA-PANASCO MORALES, G., «La responsabilidad penal de las personas jurídicas: algunas cuestiones sobre el Compliance y la protección de datos», en La ley mercantil, 2019, 3.

MARCOS AYJÓN, M., «La protección de datos de carácter personal en la justicia penal», 2017.

MARTÍNEZ MARTÍNEZ, R., «El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto», en GARCÍA MAHAMUT, R./TOMÁS MALLÉN, B. (Dirs.), El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales, 2019, 311-342.

ORDÓÑEZ PINEDA, L., «Protección de datos personales y responsabilidad proactiva», en CUICIID 2019: Congreso universitario internacional sobre la comunicación en la profesión y en la Universidad de hoy, 2019, 536.

RODRÍGUEZ AYUSO, J. F., «Protección de datos personales en el contexto de la Covid-19: legitimación en el tratamiento de datos de salud por las Administraciones Públicas», en Revista Catalana de Dret Públic, 2020, 3.

ROMEO RUIZ, A., «La responsabilidad proactiva de las Administraciones Públicas en la protección de datos personales», en Revista Vasca de Gestión de Personas y Organizaciones Públicas, 2020, 138-153.

ROTONDO TORNARÍA, F., «El principio de responsabilidad y el reglamento europeo de protección de datos», en Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época), 2019, 135-152.

SIERRA LÓPEZ, M. V., «Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 1981/2», en DEL CARPIO DELGADO, J. (Coord.), Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal, 2018, 133-186.

VENTURA PÜSCHEL, A., «El dolo penal», en MANJÓN-CABEZA OLMEDA, A./ VENTURA PÜSCHEL, A./QUINTERO OLIVARES, G./CARBONELL MATEU, J. C./MORALES PRATS, F./GARCÍA RIVAS, N./ÁLVAREZ GARCÍA, F. J. (Dirs.), Esquemas de teoría jurídica del delito y de la pena (corregida y adaptada a la LO 1/2015, de 30 de marzo), 2018, 83-90.