Revista de Estudios Europeos
Nº 78, julio-diciembre, 2021, 239-254
ISSN: 2530-9854. http://www.ree-uva.es/

PROTECCIÓN DE DATOS Y ADAPTACIÓN DEL DEBER DE DILIGENCIA[1]

DATA PROTECTION AND THE ADAPTATION OF THE DUTY OF DILIGENCE

Jesús QUIJANO GONZÁLEZ
Universidad de Valladolid

Resumen: La reciente normativa de protección de datos, tanto en el nivel comunitario como en el nacional, ha desplegado sobre quienes se consideran responsables o encargados del tratamiento un conjunto de obligaciones, generales y particulares, que constituyen con toda claridad una parte relevante del contenido actual del deber de diligencia de los administradores de las sociedades que, de forma habitual y en mayor o menor cantidad, acceden a datos de las personas físicas con las que se relacionan en el ejercicio de su actividad. A la vez, el recurso a datos útiles para la adopción de decisiones empresariales puede constituir también una manifestación del deber de diligencia, que comprende también del derecho/deber de disponer de información adecuada para el desempeño del cargo.

El presente trabajo tiene como objeto principal analizar el régimen de la protección de datos, en sus diversos aspectos (sujetos afectados, obligaciones impuestas, excepciones de tratamiento, responsabilidad por infracciones) para ponerlo en relación con el citado deber de diligencia y establecer el ámbito de responsabilidad que puede derivar, tanto para las sociedades que acceden a datos y los almacenan o utilizan, como para sus administradores.

Palabras clave: Protección de datos; tratamiento de datos; responsables y encargados del tratamiento; obligaciones; derechos digitales; deber de diligencia; responsabilidad; infracciones y sanciones.

Abstract: The recent data protection regulations, both at the community and national level, have deployed a set of obligations, general and particular, on those who are considered responsible or in charge of the treatment, which clearly constitute a relevant part of the current content of the duty of diligence of the administrators of the companies that, on a regular basis and to a greater or lesser extent, access the data of the natural persons with whom they relate in the exercise of their activity. At the same time, the use of useful data for the adoption of business decisions may also constitute a manifestation of the duty of care, which also includes the right / duty to have adequate information for the performance of the position.

The main purpose of this work is to analyze the data protection regime, in its various aspects (affected subjects, imposed obligations, treatment exceptions, responsibility for infractions) to put it in relation to the aforementioned duty of care and establish the scope of responsibility that may arise, both for the companies that access data and store or use it, as well as for their administrators.

Keywords: Data Protection; data treatment; responsible and in charge of the treatment; obligations; digital rights; duty of care; responsibility; infringements and sanctions.

---

1 Este trabajo se ha realizado al amparo del Proyecto de Investigación: "El impacto de la economía digital en el Derecho de la Competencia y la Distribución: del Big Data al Blockchain", (RTI2018-094201-B-C22), del Ministerio de Ciencia, Innovación e Universidades.

Sumario: 1. Introducción y planteamiento general. 2. El alcance actual del deber de diligencia de los administradores: breve indicación. 3. Los aspectos relevantes de la protección de datos. 3.1. El concepto de tratamiento de datos en las fuentes reguladoras. 3.2. Los sujetos afectados: responsables y encargados del tratamiento de datos. 3.3. Las obligaciones impuestas. 3.3.1. Los principios y las obligaciones generales. 3.3.2. La garantía de los derechos digitales. 3.3.3. Los Códigos de conducta y la certificación. 3.4. Supuestos especiales con excepción de tratamiento. 3.5. La específica responsabilidad: infracciones y sanciones. 4. Consideración final: deber de diligencia, tratamiento adecuado de datos y responsabilidad de administradores.

1. Introducción y planteamiento general

El impresionante desarrollo que ha tenido el proceso de digitalización prácticamente en todos los ámbitos económicos y sociales ha traído consigo una creciente preocupación por la acumulación de información sobre las personas en manos de operadores de la más variada naturaleza. En efecto, continuamente estamos introduciendo en la red, como consecuencia de la frecuente actividad que realizamos en ella con los más diversos fines (transaccionales, de comunicación, publicitarios, informativos, de búsqueda, etc.), datos que la propia tecnología permite almacenar, clasificar y utilizar. De modo que no es extraño que la protección de esos datos personales se haya convertido en uno de los objetivos más insistentemente reclamados, hasta el punto de constituir uno de los principales fundamentos de los derechos subjetivos de última generación.

A ese movimiento responde la profusa legislación que se ha desplegado durante la última década y que, en nuestro entorno, combina disposiciones comunitarias y nacionales de similar estructura y contenido. De ellas deriva, como tendremos ocasionar de examinar con detalle, un amplio marco de nuevas obligaciones para las empresas que realizan tratamiento de datos en cualquiera de sus variantes, susceptible de generar responsabilidad por incumplimiento, por infracciones o por daños, tanto para las propias entidades, generalmente con forma de sociedad mercantil, como eventualmente para sus administradores y directivos. Una especie de nueva exigencia de "compliance", requiere de ellos adoptar medidas técnicas y organizativas de protección de datos, adecuadas y suficientes. Y es en esa perspectiva donde entra en relación tal requerimiento para cumplir debidamente con el deber de cuidado y de control en esta delicada materia, con la pauta de conducta que deben aplicar quienes están llamados a tomar las decisiones directivas en cada caso. Dicho en otros términos, la protección de datos y su régimen legal se han convertido tambiénen un elemento relevante en la integración del contenido del deber de diligencia de administradores de las sociedades y directivos de las empresas.

El presente trabajo pretende, pues, poner en contacto el doble ámbito al que se hace referencia: en primer lugar, estableciendo como punto de partida el alcance que el deber de diligencia de los administradores tiene en la actualidad, tomando como base el Texto Refundido de la Ley de Sociedades de Capital en este punto, pues ésta es la base general y común de atribución de obligaciones que, teniendo distinta procedencia y contenido, recaen en última instancia en el órgano societario que, por su competencia directiva, asume entre sus funciones la de cumplir los mandatos dirigidos a la persona jurídica administrada, con el correspondiente efecto de responsabilidad cuando el incumplimiento de su deber de diligencia trae consigo el incumplimiento de las obligaciones que recaen sobre la entidad; a continuación, examinando con mayor detalle los aspectos relevantes del régimen vigente de la protección de datos (sujetos afectados; obligaciones impuestas en el tratamiento de datos; supuestos especiales de excepción; responsabilidad derivada), pues es este conjunto de aspectos el que se proyecta sobre la esfera de atribuciones de los administradores, integrando el contenido del deber de diligencia de la misma forma en que lo hacen las muy diversas obligaciones legales, estatutarias, reglamentarias, etc., que recaen sobre ellos.

Ocurre, en todo caso, que el alcance obligacional del tratamiento de la protección de datos tiene una peculiaridad muy especial, directamente relacionada con la naturaleza atribuida a esta materia. Tanto la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, como el Reglamento 2016/679, de 27 de abril de 2016, igualmente relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos

datos, consideran que la citada protección es un derecho fundamental, como así lo afirman en su respectivo Considerando primero, declaración que reproduce el Preámbulo de la Ley española (Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales), con referencia al artículo 18, 4, de la propia Constitución, que, con una formulación ciertamente novedosa, indica ya que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Esta superior dimensión de la protección de datos estaba ya presente en los antecedentes próximos de la actual normativa, tanto en el ámbito comunitario (Directiva de 24 de octubre de 1995), como en el nacional (Ley de 29 de octubre de 1992, y Ley Orgánica de 5 de diciembre de 1999, elaborada para la trasposición de la citada Directiva) y había sido igualmente destacada en la jurisprudencia, tanto del Tribunal de Justicia de la Unión Europea, como de nuestros Tribunales Supremo y Constitucional (la Sentencia de éste, de 4 de mayo de 1998, ya había destacado el carácter de derecho fundamental de las personas físicas la protección de sus datos).

De tal consideración, que invocaba como objetivo de la regulación "contribuir a la plena realización de un especial de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas" (así lo proclama el Considerando 2 del Reglamento comunitario), derivan necesariamente efectos singulares en la técnica de protección jurídica, como corresponde a un derecho calificado como fundamental, de manera que el tratamiento de datos se construye sobre un principio básico de consentimiento de la persona interesada. Tal consentimiento, según lo define el artículo 4, 11), del propio Reglamento, debe revestir los caracteres de una "manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen". Curiosamente, en esa llamada "paradoja de la privacidad", donde se combina una elevada preocupación por la utilización de datos personales con la frecuente inconsciencia mecánica con que se consiente en su tratamiento, se sitúa hoy el indefinido espacio de la protección de datos. Y es precisamente ahí donde entra en juego el deber de diligencia de quienes ejercen el poder de dirección de los sujetos jurídicos a los que se atribuye la condición de "responsables y encargados del tratamiento", sobre los que recaen las obligaciones de disponer de programas y políticas adecuadas de protección. Procede entonces, como ya se anticipó, una breve referencia a la configuración actual del deber de diligencia y un examen que en su plural contenido obligacional tiene el régimen vigente de la protección de datos.

Más allá de esta perspectiva de la relación entre el deber de diligencia y la protección de datos, hay que considerar también, aunque no sea el objeto central de este análisis, que cumplir debidamente el deber de diligencia, e incluso invocar el amparo de la protección de la discrecionalidad empresarial frente a eventuales daños derivados de decisiones estratégicas y de negocio, exige cada vez con más frecuencia en la actualidad la utilización de datos, especialmente los almacenados a gran escala en la categoría de big data. No es, pues, descartable, que la exigencia de responsabilidad pueda ser procedente por infracción del deber de diligencia, o por no concurrir los presupuestos de protección de la discrecionalidad con efecto exoneratorio, en determinadas situaciones en que la adopción de una decisión perjudicial para la sociedad pudo haberse evitado de haber contado con la información adecuada que hubieran aportado los datos disponibles mediante un tratamiento adecuado y razonable, lo mismo que si no se adoptó una decisión que debió adoptarse teniendo en cuenta dichos datos y tal omisión evidencia un nexo causal efectivo con el daño derivado en este caso, sea por pérdida de competitividad de la sociedad, sea no aprovechamiento de una oportunidad nítidamente favorable.

2. El alcance actual del deber de diligencia de los administradores: breve indicación

El sometimiento de la actuación de los administradores de sociedades a pautas de conducta relativamente estandarizadas siempre estuvo presente en la legislación societaria a través de la remisión a estereotipos generales formulados con suficiente amplitud. Así fue la invocación de la "diligencia del ordenado comerciante y del representante leal", que contenía el artículo 79 de la Ley de Sociedades Anónimas de 1951, traída de la Ley alemana de 1937 y adaptada con cierta confusión entre dos deberes fiduciarios, la diligencia y la lealtad, que aparecían mezclados como si fueran una doble dimensión de un mismo deber de comportamiento. El artículo 127 del Texto Refundido de 1989 se limitó a sustituir al

comerciante por el empresario, manteniendo la misma fórmula unificada de deber de diligencia y añadiendo una mención específica al deber de secreto, como así lo hizo también la reforma de 2003, que, sin embargo, introdujo como deber específico de cada administrador el de "informarse diligentemente sobre la marcha de la sociedad", a la vez que los nuevos artículos 127 bis, ter y quáter, diferenciaban respectivamente los deberes de fidelidad ("cumplir los deberes impuestos por las leyes y los estatutos con fidelidad al interés social, entendido como interés de la sociedad"), los deberes de lealtad, ya con un listado que mezclaba cláusulas generales y enumeración casuística, y el deber de secreto, más detallado que en la formulación anterior.

El Texto Refundido de la Ley de Sociedades de Capital, de 2010, configuró por primera vez los deberes de los administradores diferenciando formalmente el deber de diligencia y el deber de lealtad en los artículos 225 y 226. El artículo 225, referido ahora al "deber de diligente administración", lo seguía formulando como el deber de desempeñar el cargo con la diligencia de un ordenado empresario, a la vez que mantenía la mención específica al deber de cada administrador de informarse diligentemente de la marcha de la sociedad. Para el deber de lealtad se conservaba la cláusula general de "desempeño del cargo como un representante leal en defensa del interés social, entendido como interés de la sociedad", añadiendo el cumplimiento de los deberes impuestos por las leyes y los estatutos, referencia más propia del deber de diligencia, como así quedaría de manifiesto en la posterior reforma.

En efecto, sobre esta estructura de los deberes fiduciarios de los administradores incidió de manera importante la reforma operada por la Ley de 3 de diciembre de 2014, para la mejora del gobierno corporativo, que introdujo importantes novedades, algunas de ellas de especial interés para la integración de la materia que aquí nos ocupa, la protección de datos, en el contenido actualizado del deber de diligencia.

En primer lugar, la diligencia del ordenado empresario aparece ahora con una doble funcionalidad: como venía ocurriendo tradicionalmente, sigue siendo una pauta de conducta general en el desempeño del cargo, que permite evaluar los actos u omisiones de los administradores por contraste por lo que, en términos ideales, hubiese sido exigible al estándar de comportamiento de un ordenado empresario, teniendo en cuenta las circunstancias del caso concreto (el momento, el lugar, el contexto, la sociedad en cuestión, etc.); pero también la diligencia exigible opera como modalidad de cumplimiento de los demás deberes, más concretos, impuestos por las leyes y los estatutos (incluidos los reglamentos societarios), lo que permite valorar si tal cumplimiento ha sido suficiente, oportuno, tempestivo, adecuado, etc.

En segundo lugar, la fórmula legal permite una considerable graduación en cuanto al alcance, contenido, intensidad, etc., con que el deber puede ser exigible a cada administrador, teniendo en cuenta la diversidad de posiciones que cada uno de ellos puede ocupar en las distintas modalidades de composición, organización interna y funcionamiento de la administración societaria. El artículo 225 invoca en concreto "la naturaleza del cargo y las funciones atribuidas" a cada uno de los administradores como factores a considerar en la citada graduación, sin duda pensando en las modalidades más habituales de conformación interna del órgano administrativo cuando adopta la forma de consejo de administración y, bien sea utilizando la amplia disponibilidad de auto organización y delegación que la ley concede, bien cumpliendo las disposiciones legales obligatorias para ciertos tipos de sociedades (las sociedades cotizadas principalmente), establece una estructura en la que la diversificación de cargos y funciones permite, en efecto, modular y adecuar la pauta de diligencia exigible en cada caso. Como es bien sabido, la distinción entre los niveles de dirección y supervisión, entre consejeros ejecutivos y consejeros que no lo son, sean independientes o de otro tipo, entre funciones delegadas y funciones no delegadas e indelegables, funciones concentradas y distribuidas, etc., orientan con frecuencia esos modelos organizativos; pero también la posición propia de cargos unipersonales dentro del consejo, la existencia de comisiones especializadas, obligatorias o voluntarias, las fórmulas de relación entre el consejo de administración de la sociedad y el comité de dirección de la empresa, etc., contribuyen a perfilar modelos organizativos y funcionales donde es igualmente posible adecuar el deber de diligencia a los casos concretos.

Por otra parte, el deber de diligencia, más allá de la cláusula general que acaba de comentarse, tiene ahora dos manifestaciones legales expresas con importante incidencia en ese objetivo de incorporación de las exigencias derivadas de la protección de datos a su contenido obligacional.

En primer lugar, conforme al artículo 225, 2, "los administradores deberán tener la dedicación adecuada y adoptarán las medidas precisas para la buena dirección y el control de la sociedad"; ambos mandatos suponen, en efecto, que los administradores deben adoptar una actitud activa en el desempeño del cargo, no sólo mediante esa adecuada dedicación, que permite valorar el grado de atención, tiempo, etc., dedicado a su ejercicio, teniendo en cuenta de nuevo a este respecto el cargo ocupado y las funciones atribuidas, sino también adoptando medidas, si el administrador tiene capacidad para ello, o, en su caso, tomando iniciativas, presentando propuestas, suscitando debates, etc., en todo lo que estime necesario para esa "buena dirección y control de la sociedad", entendiendo que bajo este amplio concepto se encuadran los distintos ámbitos que integran el desarrollo del objeto social y la correcta gobernanza de la sociedad (el buen gobierno corporativo, la evaluación y control de riesgos, el cumplimiento de las obligaciones, la prevención de daños, el análisis crítico del desempeño, etc.). No se olvide que, en última instancia, los administradores disponen de legitimación para impugnar acuerdos del consejo, en los términos del artículo 251, y que puede haber ocasiones en que adoptar esta medida, si se dan determinadas circunstancias de las que derivan causas de impugnación suficientemente estimables, constituya una exigencia razonable en cumplimiento de esta manifestación del deber de diligencia expresamente prevista en la ley.

En segundo lugar, el apartado 3 de este mismo artículo 225, recogiendo el deber de informarse diligentemente de la marcha de la sociedad que ya constaba en el texto anterior, ha precisado su alcance con mención a la doble dimensión, de deber y de derecho, que la disponibilidad de la información tiene, con alcance individualizado, para los administradores en el desempeño de sus funciones. En efecto, la versión resultante de la reforma combina "el deber de exigir y el derecho de recabar de la sociedad", y hace objeto de ambos "la información adecuada y necesaria que le sirva para el cumplimiento de sus obligaciones", lo que supone que la extensión del contenido, tanto del deber como del derecho, vuelve a relacionarse con "el desempeño de sus funciones" (ese es el inciso inicial del precepto, referido al administrador en cada caso) y "el cumplimiento de sus obligaciones" (esta es la finalidad expresa del cumplimiento del deber y del ejercicio del derecho de información), de manera que la adecuación y la necesariedad de la información exigida o recabada habrá de valorarse en ese contexto de funciones y obligaciones. Más aún, la indudable expresividad de los términos del precepto (exigir y recabar como contenido del deber y del derecho de cada administrador) pone de relieve una vez más el carácter dinámico del deber de diligencia: el administrador no sólo tiene el derecho de solicitar, pedir, reclamar, etc., la información que considere adecuada y necesaria; también tiene el deber de hacerlo cuando lo estime conveniente, y los propios vocablos elegidos (otra vez "exigir y recabar") dan idea de la intensidad con que el precepto legal ha querido evidenciarlo. Obviamente, tanto la adecuación como la necesariedad suponen también un límite a la exigencia en el doble sentido de lo que puede ser requerido por el administrador y lo que debe ser proporcionado por la sociedad, a fin de prevenir un alcance excesivo del deber y un ejercicio abusivo del derecho, remitiendo a la decisión del presidente del consejo, o de éste en pleno, o de terceros a los que esté previsto acudir como instancia neutra de determinación objetiva de la procedencia de lo solicitado. Pero también hay que señalar que, ni el deber de exigir, ni el derecho a recabar, agotan toda la dimensión de la información; también hay derecho a ampliar, a contrastar, a investigar, la información proporcionando, incluso requiriendo auxilio de experto, etc., como hay deber de tomar conocimiento de ella, de no usarla para otros fines ajenos al desempeño del cargo, de compartirla cuando se disponga de una información individualmente obtenida, etc., pues cualquiera de estas variantes forman parte del deber de diligencia del que emana este decisivo derecho/deber de información de los administradores.

Recientemente, con ocasión de la trasposición de la Directiva de 17 de mayo de 2017, relativa al fomento de la implicación de los accionistas en las sociedades cotizadas, se ha añadido en el apartado 1 del artículo 225 de la LSC un inciso final, ciertamente discutible en cuanto a su relación con el deber de diligencia. Se refiere la adición al deber de los administradores de "subordinar, en todo caso, su interés particular al interés de la empresa", y es obvio que, si alguna relación ha de establecerse entre tal subordinación y los deberes de los administradores, el contacto se produce con el deber de lealtad y con la obligación de evitar las situaciones de conflicto de interés; pero todo ello ya está contemplado, tanto en la cláusula general del artículo 227, donde justamente se menciona el interés de la sociedad, que no el de la empresa, como objetivo que deben perseguir los administradores en el desempeño del cargo, como en el listado de obligaciones que concretan el deber de lealtad en el artículo 228 y en los supuestos particulares de conflicto de interés del artículo 229, donde la subordinación del interés particular de los

administradores al interés social, que es un concepto más expresivo que el del interés de la empresa, constituye el fundamento de la regulación de esos supuestos.

Más allá de este ámbito general del deber de diligencia en su formulación legal, debe recordarse también que el vigente Código de Buen Gobierno, auspiciado por la CNMV en 2015 para adaptarlo a la citada reforma legal de 2014 y actualizado más recientemente en 2020, específico para las sociedades cotizadas, pero con virtualidad suficiente para poder ser voluntariamente seguido en otras sociedades, contiene recomendaciones específicas , tanto en relación con la dedicación de los consejeros (25 a 28), como con la información suficiente y adecuada (29 a 32), con interesantes precisiones, útiles para mejor perfilar el contenido del deber de diligencia en este doble aspecto.

Finalmente, es de destacar que la reforma de 2014 incorporó a la LSC una regla de especial importancia como lo es la denominada "protección de la discrecionalidad empresarial", versión particular de la conocida "bussines rule", tal como está formulada en el artículo 226. Como es sabido, la regla tiene por finalidad considerar cumplido el estándar de diligencia en la adopción de determinadas decisiones estratégicas y de negocio, siempre que se cumplan determinados requisitos (actuación de buena fe, ausencia de interés personal en el asunto, información suficiente y procedimiento de decisión adecuado), de modo que, si concurren, la protección concedida tendrá efecto exoneratorio frente a eventuales responsabilidades que pudieran exigirse por los daños derivados de esas decisiones. Ahora bien, si se plantea la eventualidad de que el citado principio pudiera amparar decisiones en materia de protección de datos que constituyan infracción legal por incumplimiento de obligaciones, es evidente que el efecto exoneratorio no tiene aplicación en este ámbito; no se trata de "decisiones estratégicas o de negocio, sujetas a la discrecionalidad empresarial", que es el terreno natural de aplicación de la regla , sino del cumplimiento de obligaciones legales, canalizadas a través del deber de diligencia, sin perjuicio de que el contenido de éstas sea más o menos preciso, o conceda mayor o menor margen de elección de medidas protectoras en el tratamiento de los datos, siempre desde la perspectiva del derecho de los interesados. Se trata, pues, de un ámbito muy distinto al que el artículo 226 configura como "espacio de aplicación" de esa protección de la discrecionalidad empresarial que el precepto contempla con el fin de evitar la penalización del razonable riesgo empresarial implícito en la adopción de determinadas decisiones económicas.

Expuesto el alcance del deber de diligencia de los administradores, procede abordar los aspectos propios de la protección de datos que constituyen elementos esenciales para determinar el contenido de dicho deber en esta materia.

3. Los aspectos relevantes de la proteccion de datos

El régimen jurídico de la protección de datos, ciertamente amplio y detallado en su desarrollo normativo, se organiza principalmente en torno a un conjunto de aspectos relevantes que tienen especial incidencia a la hora de ponerlo en relación con los deberes que han de ser cumplidos por quienes asumen la responsabilidad de tal protección. Hay aspectos subjetivos, referidos a las personas físicas o jurídicas afectadas, y aspectos objetivos, referidos a las obligaciones que se imponen para garantizar los derechos de los interesados; hay casos en los que opera, matizadamente y con límites, algún tipo de excepción que facilita la licitud del manejo de los datos, y hay incumplimientos que constituyen infracción, con la consiguiente imputación de responsabilidad que conduce a la imposición de sanciones. Todo ello se configura a partir del supuesto de hecho, que es el objeto central de la regulación; esto es, del "tratamiento de datos", como categoría fáctica en torno a la cual toman forma los aspectos indicados. Convendrá, pues, fijar el alcance de este concepto nuclear, antes de examinar los aspectos indicados, tomando como referencia las distintas fuentes reguladoras donde aparece definido.

3.1. El concepto de tratamiento de datos en las fuentes reguladoras

Las fuentes reguladoras de la protección de datos en la actualidad presentan el doble nivel que se indicó anteriormente: de un lado, la normativa comunitaria (la Directiva y el Reglamento, con igual fecha de publicación, 27 de abril de 2016), con la que se pretendía alcanzar el doble objetivo de armonizar los derechos nacionales mediante la trasposición de la Directiva y, a la vez, de disponer de un derecho

comunitario uniforme y de aplicación directa en toda la Unión mediante la aprobación del Reglamento.; de otro lado, la normativa nacional, principalmente integrada por la Ley Orgánica de 5 de diciembre de 2018, de protección de datos personales y garantía de los derechos digitales, obviamente influida, con notable intensidad, por las disposiciones comunitarias. Ambos niveles han de ser tomados como base para la exposición de los aspectos del régimen jurídico en la materia, comenzando por el propio concepto de "tratamiento de datos" como fenómeno que se expresa en muy variadas manifestaciones y que agrupa múltiples actividades en torno a las que se concentran los riesgos de ilicitud por incumplimiento de las obligaciones de protección y de perjuicio a los interesados.

Tal y como aparece descrito en los listados de "definiciones" que habitualmente preceden a las normas comunitarias, el concepto de tratamiento se ha configurado como una amplia enumeración de "operaciones, o conjunto de operaciones, que se pueden realizar sobre datos personales, o sobre conjuntos de datos personales, ya sea por procedimientos automatizados o no". Esa enumeración es ciertamente exhaustiva, como fácilmente se aprecia en la citada definición (artículo 3, 2, de la Directiva, y 4, 2, del Reglamento): incluye "la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". Ninguna actuación imaginable que tenga por objeto los datos personales queda fuera de tan prolija enumeración, ni del concepto de tratamiento que constituye la base objetiva de las obligaciones de protección y del sometimiento al control legal.

De esos procedimientos automatizados de tratamiento, que sin duda constituyen una de las modalidades más relevantes en el entorno digital donde se introducen y recopilan los datos personales, destaca el que tiene por finalidad la "elaboración de perfiles", objeto también de una amplia definición normativa. Se trata de "toda forma de tratamiento automatizado de datos personales consistente en utilizar esos datos para evaluar determinados aspectos personales de una persona física, y en particular para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". Es evidente que esta técnica de elaboración de perfiles concentra el que probablemente sea el mayor riesgo potencial de acceso al ámbito personal y a la intimidad; tal peligrosidad, como tendremos ocasión de comprobar, hace que también sea el objeto más directo de la protección de datos en todo lo relativo a la garantía de los derechos digitales de las personas.

Finalmente, a esa amplitud de operaciones que pueden considerarse tratamiento de datos hay que añadir también la propia amplitud del concepto de "datos personales", igualmente recogido como primera referencia en el listado de definiciones de los textos comunitarios. Se trata de "toda información sobre una persona física identificada o identificable", a la que pueda atribuirse un "elemento identificador", sea "un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". Incluso algunos de estos datos (concretamente los genéticos, los biométricos y los relativos a la salud) tienen luego su propia definición, que contribuye aún a una mayor amplitud en la extensión del concepto.

Del tenor de este conjunto de definiciones, fácilmente se aprecia que la técnica empleada en su configuración es la del listado ejemplificativo, materializado en enumeraciones amplias y detalladas, que tampoco pueden considerarse absolutamente cerradas o exhaustivas, en el sentido de que no quepa incluir en el concepto de tratamiento, o en el propio de datos personales, otras actuaciones, u otros elementos de identificación, más allá de los que están expresamente mencionados en la enumeración legal; de ser así, esas actuaciones quedarían fuera del control, no afectadas por las obligaciones de lícito tratamiento. Pero no es esa la intención de la norma, sino más bien la contraria; esto es, ejemplificar al máximo, pero no agotar ni las modalidades de tratamiento, ni los elementos de identificación componentes de los datos personales, como bien se deduce de la propia estructura de los listados, incluso en el aspecto gramatical, además de la finalidad jurídica.

3.2. Los sujetos afectados: responsables y encargados del tratamiento de datos

Los sujetos a los que la normativa reguladora de la protección de datos impone las obligaciones relacionadas con el tratamiento aparecen identificados con una terminología ciertamente singular, que

trata de diferenciar las funciones asumidas, teniendo en cuenta la posición que ocupan en el desarrollo de las actividades que están encuadradas en el amplio espectro antes mencionado. A tal efecto, tanto la Directiva, como el Reglamento (artículos 3 y 4, respectivamente), incluyen como sujetos principales al "responsable" y al "encargado" del tratamiento, a los que luego se añaden el "destinatario" y el "delegado", con determinadas funciones propias.

El "**responsable del tratamiento"**, tal como aparece definido, puede ser "cualquier persona física o jurídica, autoridad pública, servicio u otro organismo, que, solo o junto con otros, determina los fines y medios del tratamiento"; se trata, pues, del "responsable en última instancia" al que quepa imputar las decisiones relevantes en materia de protección. Eso es lo que se deriva de la principal obligación que se le impone, como luego se detallará, consistente en "aplicar medidas técnicas y organizativas apropiadas", a fin de garantizar y poder demostrar que el tratamiento es conforme a lo exigido; así lo declaran los artículos 24 y 25 del Reglamento, que incluye entre esas medidas, también a cargo del responsable, "las oportunas políticas de protección de datos". La misma atribución realiza el artículo 28 de la Ley española, tomando, a su vez, la referencia del artículo 19 de la Directiva, teniendo en cuenta, además, que es posible que dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento, lo que conduce a la "corresponsabilidad" expresamente prevista, tanto en el Reglamento (artículo 26), como en la Ley nacional (artículo29); más aún, la Directiva y el Reglamento han previsto, en sus artículos 23 y 29, que cualquier persona que tenga acceso a datos, actuando bajo la autoridad del responsable, solo pueda someterlos a tratamiento siguiendo instrucciones de éste, salvo que esté obligado a hacerlo por disposiciones comunitarias o nacionales, lo que debe interpretarse como un reconocimiento explícito de esa atribución última de decisiones y de responsabilidad por el cumplimiento de las obligaciones de tratamiento adecuado.

El "**encargado del tratamiento"**, por su parte, viene definido como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable". Esta "posición subalterna" está desarrollada luego en detalle en los artículos 28 del Reglamento y 22 de la Directiva, con criterios propios de una relación de colaboración cualificada por la subordinación: el responsable lo es también de una elección adecuada del encargado y éste no puede hacerse sustituir por otro sin autorización previa del responsable, debiendo establecerse tal relación por medio de un contrato especial, cuyo contenido está ampliamente delimitado en esos preceptos, a los que también remite el artículo 33 de la Ley española, que, a su vez, prevé que el encargado será considerado responsable cuando establezca relaciones con los afectados en nombre propio y sin que conste que actúa por cuenta de otro, aunque haya un contrato, o cuando utilice los datos para sus propias finalidades.

Tanto el responsable como el encargado pueden no estar establecidos en la Unión, aplicándose entonces el Reglamento en los términos que indica el artículo 3, siendo en tal caso obligatoria la designación de un representante, con las funciones que le asigna el artículo 27.

El **"delegado de protección de datos"**, por su parte, constituye una figura también obligatoria que los responsables y encargados deben designar, de entre su propio personal o como profesional externo, para que, entre otras funciones de asesoramiento y supervisión, actúe como interlocutor ante la autoridad de control, en los términos que contemplan tanto el Reglamento (artículos 37 a 39), como la Directiva (artículos 32 a 35), y recoge también la Ley española (artículos 34 a 37), enumerando de forma expresa un conjunto de entidades que, en todo caso, deben disponer de la figura del delegado y confirmando esa interlocución ante la Agencia Española de Protección de Datos y las autoridades autonómicas competentes, pudiendo intervenir en caso de reclamación ante ellas.

Finalmente, aparecen también mencionados en los listados de definiciones otros sujetos, con intervención más secundaria, como es el caso de los "destinatarios", a quienes se comunican datos, los "interesados", que son las personas físicas a quienes se refieren los datos, o los "terceros", como término genérico para designar a quienes no son interesados, ni responsables, ni encargados, ni autorizados para el tratamiento, y, a pesar de ello, pueden asumir alguna obligación derivada de la disposición de datos.

La posición de los diversos sujetos enumerados como de referencia (principalmente responsables y encargados) puede ser ocupada por cualquier persona, física o jurídica, pero lo más habitual será la presencia de una empresa en tal condición. Esa es la razón por la que, en el propio listado de definiciones del Reglamento, aparezca una referencia precisamente dedicada a establecer un **concepto de empresa** deliberadamente amplio: "persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen

regularmente una actividad económica"; concepto al que acompaña otro no menos amplio de "**grupo empresarial**", que alcanza a todo "grupo constituido por una empresa que ejerce el control y sus empresas controladas". Obviamente, el citado concepto de empresa no admite exclusión: alcanza a empresarios individuales, sociedades de todo tipo, pymes y grandes empresas cotizadas, etc., sin limitación ni sectorial por la actividad, ni por el tamaño, ni por ninguna otra circunstancia, y sea cual sea su relación con el tratamiento de datos, desde un almacenamiento mínimo, hasta la disposición del control de plataformas de acumulación a gran escala de "big data", o de motores de búsqueda, etc.

Por encima de este entramado de sujetos se sitúan, en fin, las instancias de supervisión pública, autoridades de control independientes, en los distintos niveles donde se establece la protección de datos. El Reglamento contiene un régimen muy detallado en los artículos 51 a 76, donde se contiene un marco de competencias, funciones y poderes de las autoridades de control, con unas reglas de cooperación entre ellas, y se crea un "Comité europeo de protección de datos", como organismo propio de la Unión. El mismo planteamiento recoge la Directiva, en los artículos 41 a 51, como también la Ley española, que dedica a la Autoridades de protección de datos (Agencia española y autoridades autonómicas) su Título VII, artículos 44 a 62, siguiendo ese mismo modelo comunitario.

3.3. Las obligaciones impuestas

La finalidad última de la regulación de la protección de datos es la de establecer un marco de obligaciones y normas de conducta que deben observar los sujetos a los que se considera responsables o encargados del tratamiento. Ese conjunto de obligaciones, que constituye también el objeto del deber de diligencia de quienes administran o dirigen las entidades afectadas, está configurado en la normativa vigente con una estructura ciertamente compleja y con un contenido considerablemente abierto, sin duda reconducible a un deber general de control del tratamiento y de cuidado para asegurar la protección de los interesados. Siendo así, y con el fin de ofrecer una perspectiva sistematizada de tales obligaciones, pueden distinguirse tres aspectos que, sin perjuicio de su respectiva naturaleza particular, operan de forma conjunta y con una estrecha relación en cuanto a su incidencia jurídica. Están, en primer lugar, los principios orientadores del tratamiento y las obligaciones generales que de ellos derivan; en segundo lugar, las garantías de los derechos digitales de los interesados, que deben ofrecerse, constituyendo en tal sentido fuente de obligaciones de respeto y protección; finalmente, la posibilidad de elaborar "códigos de conducta" a los que los sujetos obligados puedan adherirse para disciplinar su actuación en el tratamiento de datos, quedando así vinculados por los deberes que formen parte del contenido del correspondiente código. Cada uno de estos tres aspectos merece una breve consideración específica.

3.3.1. Los principios y las obligaciones generales

Tanto el Reglamento, en los artículos 5 al 11, como la Directiva, ésta en forma más sintética en los artículos 4 al 11, establecen los principios relativos al tratamiento, enumerando las condiciones que éste debe reunir: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad. A la enumeración se añade, además, una regla de responsabilidad proactiva, según la cual el responsable del tratamiento es responsable del cumplimiento de esos principios y debe ser capaz de demostrarlo cuando sea necesario.

En el desarrollo de los principios es especialmente relevante el criterio con que debe valorarse la licitud del tratamiento: el artículo 6 del Reglamento menciona hasta seis condiciones, si bien es suficiente cumplir, al menos, una de ellas; de modo que basta que el interesado preste su consentimiento, con los caracteres que se mencionaron y con las particulares reglas de prueba, obtención transparente y revocabilidad, a que se refiere el artículo 7, o que el tratamiento sea necesario para ejecutar un contrato o cumplir una obligación legal, para proteger intereses vitales del interesad o de otra persona, para satisfacer un interés público, o un interés legítimo del responsable o de un tercero, salvo que deban prevalecer los intereses del afectado, especialmente en el caso de la infancia, que el artículo 8 eleva hasta los 16 años (los Estados pueden rebajarlo hasta 13), edad a partir de la que un menor puede prestar consentimiento para un tratamiento lícito. En todo caso, el tratamiento tiene especialidades más particulares cuando se refiere a datos sobre condenas penales (artículo 10 del Reglamento y 6 de la

Directiva), como también la prohibición de tratamiento es más estricta cuando se refiera a los datos que menciona el artículo 9 del Reglamento, relativos al origen étnico, a la opinión política, convicción religiosa o filosófica, afiliación sindical, o a datos genéticos, de la salud, o de la orientación sexual, sin perjuicio de las excepciones que el propio precepto señala, que alcanzan desde el consentimiento explícito del interesado hasta la necesidad con fines de archivo en interés público, para la investigación o la estadística.

Con base en este modelo de principios, la Ley española formula su propio sistema, mencionando como tales, en los artículos 4 al 10, la exactitud y actualización de los datos, el deber de confidencialidad, el consentimiento del afectado, manifestado con voluntad libre, específica, informada e inequívoca, y con la especialidad de los menores de edad, con el límite de los 14 años, la licitud derivada de obligación legal, interés público o ejercicio de potestades públicas, y el reconocimiento de las categorías singulares de los datos más relacionados con la dignidad personal, o de los datos de naturaleza penal.

Las obligaciones generales del responsable del tratamiento están formuladas en todos los textos (artículo 24 del Reglamento, 19 de la Directiva y 28 de la Ley española) con el mismo grado de amplitud: se trata de un "deber de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa aplicable", para lo que debe disponer de las "oportunas políticas de protección de datos", si bien es cierto que en el diseño de tales medidas ha de tenerse en cuenta el estado de la técnica, el costo de aplicación, la naturaleza, ámbito, contexto y fines del tratamiento, así como la probabilidad y gravedad de los mayores riesgos, que son los derivados de situaciones de posible discriminación, fraude, daño, privación de derechos, especial vulnerabilidad, etc.

En ese contexto, adquieren especial trascendencia algunas obligaciones de contenido más concreto, diseminadas a lo largo de las disposiciones de referencia, como son la de garantizar un nivel de seguridad adecuado, que alcanza a la comunicación de la violación de datos tanto a la autoridad de control, como al propio interesado (artículos 32, 33 y 34 del Reglamento); la de evaluar el impacto sobre la protección, especialmente con ocasión de la aplicación de nuevas tecnologías en el tratamiento, incluso con consulta previa a la autoridad de control (artículos 35 y 36); la llevanza de un registro de actividades de tratamiento, con especificación de la información que debe contener (artículo 30). También la Directiva hace referencia a estas obligaciones más concretas de registro, cooperación, evaluación, consulta previa, seguridad y comunicación, en los artículos 24 a 31, e igualmente la Ley española establece como obligación la llevanza del Registro de actividades de tratamiento (artículo31), añadiendo en su artículo 32 un deber ciertamente especial como lo es el de bloqueo de datos cuando el responsable del tratamiento proceda a su rectificación o supresión.

Como ya se apuntó en el momento inicial, la configuración de estos deberes de cuidado en materia de protección de datos, y salvadas las distancias del ámbito penal en que se han incluido en relación con la responsabilidad de las personas jurídicas, guarda cierta similitud con la importancia atribuida a la implantación de modelos de organización y gestión, con medidas de supervisión, vigilancia o control idóneas para la prevención de riesgos, que el artículo 31 bis del Código penal menciona como causas de exención de dicha responsabilidad penal. El contenido y funciones de los "programas de compliance" que de ahí derivan (adopción, ejecución, supervisión, verificación periódica, etc. de los modelos de organización, gestión, prevención y control), materializados en la elaboración de protocolos y procedimientos de actuación, adaptables a las circunstancias de cada entidad, constituyen un valioso precedente para la implantación de pautas de tratamiento de la protección de datos, con favorable incidencia jurídica cuando sea oportuno. Los propios Códigos de conducta, que luego son objeto de consideración, constituyen, a estos efectos, un instrumento con el que se puede materializar tal objetivo de estandarización de pautas organizativas y de control.

3.3.2. La garantía de los derechos digitales

Los datos que constituyen el objeto del tratamiento y de la protección legal se obtienen, almacenan, procesan y utilizan principalmente en el entorno digital, lo que supone que a los interesados les sean reconocidos los llamados "derechos digitales" (derechos en la era digital, o en internet) para la defensa de sus intereses en la red. La garantía de esos derechos por parte de los operadores, a su vez responsables y encargados del tratamiento de datos, constituye también una amplia fuente de obligaciones para ellos y, en última instancia, un componente del deber de diligencia exigible a sus

órganos de administración. De nuevo en este aspecto, los textos en vigor (El Reglamento, en los artículos 12 a 22, la Directiva, en los artículos 12 a 18, y la Ley española, en los artículos 11 a 18 y 79 a 97) contienen amplias enumeraciones de derechos a las que se conectan obligaciones de garantía y protección.

El catálogo recogido en la Directiva y en el Reglamento, presenta una evidente similitud, tanto en el contenido, como en la sistemática con que está configurado. Se empieza estableciendo, como un deber de transparencia y de comunicación de los responsables, la obligación de adoptar medidas razonables para proporcionar a los interesados toda la información relativa al tratamiento de sus datos, distinguiendo si se han obtenido directamente de ellos o de un tercero, y a las formas en que pueden ejercer sus derechos. A partir de ahí, la enumeración comprende, con matices y limitaciones en algunos casos, los derechos que han alcanzado mayor notoriedad en el entorno digital, no exenta de polémica con frecuencia: el derecho de acceso del interesado a sus datos personales, el derecho de rectificación, supresión (el conocido derecho al olvido) y limitación de tratamiento, el derecho a la portabilidad de los datos, el derecho de oposición y el derecho a no ser objeto de decisiones individuales automatizadas, lo que incluye la elaboración de perfiles. Las limitaciones, por su parte, deben respetar en lo esencial los derechos, y deben ser necesarias y proporcionadas, con fundamento en "intereses generales y superiores", relacionados con la seguridad, la defensa, la investigación penal, la protección de reglas de deontología, el respeto de los derechos de terceros, etc.

Cierta peculiaridad presenta la opción sistemática de la Ley española: dedica un Título III, artículos 11 a 18, al catálogo de derechos de las personas (acceso, rectificación, supresión, limitación, portabilidad y oposición), precedido de reglas específicas sobre transparencia e información a proporcionar por el responsable del tratamiento al afectado y sobre las formas y medios para ejercer esos derechos. Posteriormente, en el Título X, artículos 79 a 97, desde la perspectiva de la garantía de los derechos digitales que debe ser ofrecida por los prestadores de servicios de la sociedad de la información y los proveedores de servicios de internet, se detalla un nuevo listado que no tiene parangón con el alcance de los textos comunitarios en este aspecto; se recogen aquí el derecho a la neutralidad en internet, el de acceso universal a internet, el de educación digital, con especial referencia a la protección de menores y de sus datos en internet, el de rectificación y actualización de informaciones, los específicos en el ámbito laboral (el de intimidad, uso de dispositivos digitales, desconexión, protección frente a la videovigilancia, grabación de sonidos y sistemas de geolocalización, con posibles garantías adicionales en la negociación colectiva), el derecho al olvido en búsquedas de internet y en servicios de redes sociales, el de portabilidad en esos mismos entornos y, finalmente, el derecho al testamento digital, referido al acceso a contenidos relacionados con personas fallecidas. Fácilmente se aprecia que este doble conglomerado de derechos proclamados con carácter más general y de deberes de garantía más específica de los considerados derechos digitales, constituye una fuente de obligaciones para los sujetos responsables y encargados del tratamiento de datos, que, por la propia naturaleza de su contenido, fundamenta un elevado nivel de exigibilidad de una diligencia especialmente cualificada, cuya infracción será susceptible de generar responsabilidad, tanto en forma de sanción administrativa, como de reparación de daños causados a los interesados.

3.3.3. Los Códigos de conducta y la certificación

Por la incidencia que pueden tener en cuanto a una más precisa delimitación del marco de obligaciones de los responsables del tratamiento y a los efectos de una mejor apreciación y valoración de su actuación, tanto el Reglamento europeo, como la Ley española, hacen referencia a dos instrumentos de especial interés como son los Códigos de conducta y los mecanismos de certificación por instituciones acreditadas. Los artículos 38 y 39 de la Ley española, más bien parcos en este aspecto, remiten al mayor desarrollo que contienen los artículos 40 a 43 del Reglamento.

Los Códigos de conducta son concebidos como un instrumento a promover por las autoridades públicas para contribuir a la más correcta aplicación de las normas de protección, adaptadas a las características específicas de los sectores de tratamiento y a las necesidades particulares de empresas de menor tamaño. Su amplio contenido puede incorporar reglas de tratamiento leal y transparente, de ejercicio de derechos de los interesados, de transferencia de datos, o de procedimientos extrajudiciales de solución de conflictos; de manera que pueden constituir un eficaz parámetro de orientación de conductas

y de medida del grado de diligencia empleada en la actuación de los responsables y en su adecuación a las pautas establecidas en el Código. Su elaboración puede ser iniciativa de asociaciones y organismos representativos de categorías de responsables o encargados del tratamiento, con adhesión voluntaria de éstos y efecto vinculante para los adheridos; pero el hecho de que el proyecto de Código, o su modificación posterior, pueda ser sometido a examen y aprobación de la autoridad de control, que se pronuncia sobre su conformidad con las normas de protección, así como la previsión en los propios Códigos de organismos de supervisión de su cumplimiento, una vez aprobados, refuerza su significación jurídica y su utilidad normativa a la hora de valorar la corrección del tratamiento de datos en los casos concretos, especialmente en el ámbito de la resolución extrajudicial de reclamaciones y conflictos.

La certificación, por su parte, junto con los sellos y marcas de protección que pueden promoverse por las autoridades públicas, pueden tener una interesante y relevante función probatoria a la hora de establecer el cumplimiento de las normas en materia de tratamiento de datos por los responsables y encargados. Expedida por un organismo acreditado, y con validez temporal, la certificación es voluntaria y se obtiene a través de un procedimiento transparente, pero, en todo caso, como lo advierte el artículo 42, 4, del Reglamento, no "limita la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento de las normas de protección y se entiende sin perjuicio de las funciones y los poderes de las autoridades de control competentes".

3.4. Supuestos especiales con excepción de tratamiento

En evidente contraposición al régimen general del tratamiento de datos, de orientación marcadamente restrictiva en su contenido obligacional para responsables y encargados, la normativa en la materia contempla también supuestos concretos en los que prima una orientación más flexible y permisiva, por lo que cabe configurarlos como excepciones de tratamiento. En la medida en que tales supuestos contribuyen indirectamente a delimitar el ámbito de la protección de datos y también, por contraste, el alcance de las obligaciones en cuyo cumplimiento ha de emplearse la diligencia exigible, procede una simple consideración sobre su significado y contenido.

El artículo 6 del Reglamento europeo, al referirse a las condiciones que permiten apreciar la licitud del tratamiento, ya contempla, junto al consentimiento del interesado, un conjunto de criterios de los que deriva ese efecto: así, la necesidad para la ejecución de un contrato en el que el interesado es parte, el cumplimiento de una obligación legal aplicable al responsable del tratamiento, la protección de intereses vitales del interesado o de otra persona física, el cumplimiento de una misión en interés público o en el ejercicio de poderes públicos conferidos al responsable, y, sobre todo, por su función de cláusula general de cierre de los supuestos de licitud, la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses, derechos o libertades fundamentales del interesado que requieran protección de datos personales, en particular si se trata de un niño. Tales condiciones vuelven luego a ser mencionadas en el artículo 49 para configurar las "excepciones para situaciones específicas" que permiten la transferencia de datos personales a terceros países u organizaciones internacionales, dentro del régimen contenido en los artículos 44 a 50, donde dicha transferencia se somete al principio de adecuación, tanto en la decisión de transferir, como en la exigencia de garantías de tratamiento correcto, así como también los artículos 85 a 91 contienen "disposiciones relativas a situaciones específicas de tratamiento", de muy variado alcance, pues, como ejemplo, se mencionan tratamientos con fines periodísticos y de expresión académica, artística o literaria, los del ámbito laboral, los de interés estadístico y de investigación científica o histórica, o, en fin los que vengan realizando las iglesias y asociaciones religiosas.

De forma más explícita, la Ley española recoge en su Título IV, artículos 19 a 27, un conjunto de "disposiciones aplicables a tratamientos concretos", referidas a supuestos de diversa naturaleza. Junto a algunos más directamente relacionados con el interés público general (así el tratamiento con fines de videovigilancia, los sistemas de información de denuncias internas, el tratamiento de datos en el ámbito de la función estadística pública, o con fines de archivo por las administraciones públicas, o en relación con infracciones y sanciones administrativas), hay otros de especial incidencia en la actividad económica y empresarial, conectados a intereses más bien privados.

Está, en primer lugar, el tratamiento de datos de contacto, de empresarios individuales y de profesionales; se trata de datos de contacto, o relativos a la función o puesto que desempeña una persona

física que presta servicios a una persona jurídica, siempre que tengan por finalidad la localización o el mantenimiento de relaciones derivadas de la prestación del servicio, así como los datos de empresarios individuales y profesionales liberales, cuando se refieran a ellos exclusivamente en esa condición y no para entablar relación con ellos como personas físicas.

Es también el caso de los sistemas de información crediticia, en los que se presume lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información, siempre que se cumplan determinados requisitos que establece el artículo 20, como son, entre otros, que los datos hayan sido proporcionados por el acreedor, que se trate de deudas ciertas, vencidas y exigibles, que se haya informado al afectado, que los datos se mantengan sólo mientras dure el incumplimiento, etc.

En tercer lugar, está el supuesto de los tratamientos relacionados con la realización de determinadas operaciones mercantiles, entre las que expresamente se mencionan las modificaciones estructurales de sociedades, la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que fuera necesario para el buen fin de la operación y se garantice la continuidad en la prestación de los servicios; supuesto que se materializa en los conocidos procesos de "due diligence" que se desarrollan con ocasión de este tipo de operaciones.

Finalmente, está el supuesto relacionado con los sistemas de exclusión publicitaria, en los que el tratamiento de datos es lícito cuando tiene por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas; a tal fin, está permitido, comunicándolo a la autoridad de control, crear sistemas de información generales o sectoriales que incluyan los datos imprescindibles para identificar a los afectados, a los que debe informarse, cuando manifiesten su deseo de acogerse a ellos, de los sistemas de exclusión publicitaria existentes.

La apreciación conjunta de estos supuestos especiales de tratamiento permite, sin duda, valorar más adecuadamente el alcance de las obligaciones, pero también la posibilidad de aplicarlos en la actividad empresarial con efectos beneficiosos, lo que puede constituir igualmente una exigencia de la vertiente activa del deber de diligencia exigible, cuyo contenido alcanza el cumplimiento de obligaciones de hacer y no hacer, en el sentido de utilizar adecuadamente el tratamiento de datos que se presume o considera legalmente lícito, con efectos beneficiosos, y de evitar actuaciones ilícitas, de incumplimiento o de cumplimiento defectuoso o insuficiente de obligaciones, con efectos perjudiciales para la entidad que tiene el carácter de responsable o encargada del tratamiento.

3.5. La específica responsabilidad: infracciones y sanciones

Como es habitual en la legislación administrativa reguladora de una determinada actividad, también la normativa de protección de datos contiene un régimen de responsabilidad específico, compuesto por reglas sobre la competencia de la autoridad de control, el procedimiento para sustanciar la responsabilidad, la tipificación de las infracciones en la materia y las sanciones que pueden imponerse.

La Directiva europea (artículos 52 a 57) hace referencia al asunto con unos mínimos principios: el derecho de los interesados a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva contra las decisiones de esa autoridad y contra el responsable o el encargado del tratamiento, derechos que pueden ejercitarse por medio de representante, así como el derecho a la indemnización de los daños y perjuicios causados por un tratamiento ilícito de sus datos; el catálogo de infracciones y las correspondientes sanciones, que deben ser efectivas, proporcionadas y disuasorias, son aspectos remitidos al ordenamiento de los Estados miembros.

De forma más explícita y detallada, el Reglamento precisa la competencia, funciones y poderes de la autoridad de control (artículos 51 a 59), entre las que expresamente se mencionan la tramitación de las reclamaciones, la realización de investigaciones, la estimación de infracciones y la imposición de sanciones, con especial atención a la coordinación entre las diversas autoridades de control y a lo que denomina "mecanismo de coherencia" para asegurar una aplicación homogénea de las normas de protección por dichas autoridades (artículos 60 a 67), objetivo en el que tiene una importante tarea el Comité europeo de protección de datos (artículos 68 a 76). Junto a ello, recoge también los derechos de reclamación y de tutela judicial efectiva (artículos 77 a 81), si bien, al contemplar el derecho a la indemnización de los daños y perjuicios causados por una infracción, lo hace sentando paralelamente el

principio de responsabilidad de quienes realizan el tratamiento de datos, como responsables o encargados, y reforzando la garantía del perjudicado con la responsabilidad solidaria de todos ellos, sin perjuicio del derecho de repetición entre ellos (artículo 82).

Pero no se limita el Reglamento a establecer esta dimensión indemnizatoria del daño causado por las infracciones del tratamiento; en aplicación de esa técnica propia del derecho administrativo sancionador, los artículos 83 y 84 contienen un régimen particular de infracciones y sanciones, que se materializa en la imposición de multas administrativas de dos posibles cuantías en función del nivel de gravedad considerado en la norma; sin perjuicio del elevado número de criterios de graduación (hasta 11 contempla el artículo 83), las multas pueden alcanzar hasta diez y veinte millones de euros respectivamente, pero, tratándose de empresas infractoras, cabe optar por esa sanción o por otra consistente en el equivalente al 2 o al 4 %, como máximo, del volumen de negocio total anual global del ejercicio financiero anterior, debiendo imponerse la de mayor cuantía. El Reglamento, en fin, encomienda a los Estados miembros completar el régimen sancionador indicado, pero no deja de advertir que, si el ordenamiento de un Estado miembro no establece multas administrativas, podrá aplicarse por las autoridades de control y por los tribunales nacionales el sistema de su propio artículo 83, para incoar e imponer la sanción.

No es este el caso de la legislación española. Nuestra ley, además de una amplia regulación de las autoridades de control (la Agencia española de protección de datos y las Autoridades autonómicas de control), a las que dedica el Título VII, artículos 44 a 62, establece los procedimientos a aplicar en caso de vulneración de la normativa de protección de datos (Título VIII, artículos 63 a 69) y, más especialmente, contiene un régimen sancionador, configurado siguiendo el modelo del Reglamento europeo, pero con un nivel de detalle mucho más preciso (Título IX, artículos 70 a 78).

Dicho régimen sancionador empieza por definir los sujetos responsables a los que se puede aplicar (responsables del tratamiento, encargados, representantes, entidades de certificación y entidades acreditadas de supervisión de los códigos de conducta), y a continuación, a la vez que remite el catálogo de infracciones al que contiene el artículo 83 del Reglamento europeo, las tipifica singularizadamente y las clasifica en las tres categorías habituales de las infracciones administrativas (muy graves, graves, leves), con plazos de prescripción respectivos de 3, 2 y 1 año. No hay, sin embargo, un desarrollo particularizado equivalente para la imposición de sanciones: el artículo 76 remite sin más al Reglamento europeo, especificando criterios de graduación de la sanción, mientras que el artículo 78 indica los plazos de prescripción de las sanciones atendiendo a su cuantía; ello supone que la autoridad sancionadora ha de acomodar la estructura de sanciones del Reglamento, configurada en torno a las categorías y supuestos que distingue el artículo 83, en sus apartados 4, 5 y 6, a la hora de aplicarlas a las categorías de infracción, por razón de la gravedad, que distinguen los artículos 72, 73 y 74. Lo que sí hace, finalmente, la Ley española es extender el régimen de infracciones y sanciones, con alguna especialidad, a las que el artículo 77 considera "determinadas categorías de responsables o encargados del tratamiento", incluyendo, entre otras, los órganos constitucionales y jurisdiccionales, la administración pública en todos sus niveles, las fundaciones del sector público, las universidades públicas, los consorcios o los grupos parlamentarios.

4. Consideración final: deber de diligencia, tratamiento adecuado de datos y responsabilidad de administradores

La perspectiva utilizada a lo largo del análisis de la legislación de protección de datos tenía como intención declarada poner en relación el deber de diligencia de los administradores de las sociedades con el cumplimiento de las obligaciones que recaen sobre éstas, como responsables o encargadas del tratamiento en los términos legales que se han ido examinando. Del incumplimiento de esas obligaciones podrá derivar para ellas una doble consecuencia negativa de carácter económico: satisfacer la correspondiente indemnización de los daños y perjuicios causados a las personas afectadas por el tratamiento ilícito o inadecuado de sus datos y asumir la sanción de multa por la infracción que le resulta imputada. Ambos conceptos suponen un daño al patrimonio social susceptible de ser repercutido a los administradores de la sociedad en aplicación del régimen de responsabilidad de éstos, previsto en los artículos 236 y siguientes de la Ley de Sociedades de Capital.

En efecto, la situación descrita es susceptible de integrar el presupuesto material para el ejercicio de la acción social de responsabilidad de la sociedad contra sus administradores; se trata de vincular causalmente el daño sufrido por la sociedad como consecuencia de haber recaído sobre ella las consecuencias patrimoniales negativas de las infracciones de tratamiento que le han sido imputadas con las acciones u omisiones ilícitas y culpables de sus administradores. Es ahí donde incide específicamente el deber general de diligencia, que obliga a los administradores a cumplir adecuadamente las obligaciones legales, como así lo expresa el artículo 225, sin perjuicio de que éstas tengan como sujeto de referencia a la sociedad administrada. Entre esas obligaciones está la de adoptar las medidas técnicas y organizativas apropiadas, que aseguren un tratamiento lícito y adecuado de datos, de manera que su incumplimiento culpable o negligente debe legitimar a la sociedad para ejercitar la acción social con el objetivo de obtener reparación del daño causado al patrimonio social que ha debido soportar tanto la indemnización a los interesados perjudicados como la multa administrativa impuesta.

Puede resultar un tanto extraño que la legislación de protección de datos no contemple la posibilidad de sanción administrativa directa y personal a administradores y directivos de la entidad infractora, como es habitual en el ámbito de la responsabilidad administrativa (así ocurre, por ejemplo, en la legislación sectorial de las entidades de crédito, o de las empresas aseguradoras, entre otros muchos supuestos, e incluso en la legislación de defensa de la competencia, donde se contempla esa opción sancionadora, compatible con la sanción a la entidad a la que se imputa la infracción, y sin perjuicio de la posibilidad de exoneración de administradores no participantes en la acción u omisión infractora). Tal circunstancia, sin embargo, no es óbice para que la sociedad pueda repercutir a sus administradores el daño por ella experimentado, siempre que concurran los presupuestos de la responsabilidad de éstos (acción u omisión ilícita y culpable, en este caso materializada en el incumplimiento de las obligaciones del tratamiento de datos, y apreciación suficiente del nexo causal entre esa conducta, que normalmente consistirá en infracción del deber de diligencia, y el daño causado a la sociedad). Más bien, el hecho de que no esté contemplada la citada sanción personal a administradores o directivos puede suponer un acicate para la pretensión de la sociedad de obtener la oportuna compensación del daño a través del ejercicio de la acción social, entendiendo que sus administradores son en última instancia los responsables a los que cabe imputar la actuación causante de ese daño que le ha sido atribuido a la sociedad por los interesados a los que ha debido indemnizar y por la autoridad de control a la que ha debido satisfacer la sanción económica.

Tampoco será descartable la posibilidad de ejercicio de la acción individual cuando quepa apreciar una lesión directa en los intereses de un tercero, en los términos en que lo contempla el artículo 241 de la Ley de Sociedades de Capital; se trataría de infracciones, no ya tanto del deber general de adoptar medidas adecuadas para el tratamiento de datos, sino de actuaciones expresamente dirigidas de forma directa a perjudicar a un determinado interesado, o que han producido directamente ese resultado. Piénsese, por ejemplo, en aquellos casos en que una deficiente custodia y control de los datos almacenados permite que terceros accedan a ellos y los utilicen para realizar actos perjudiciales para los titulares de dichos datos. En tales supuestos, el perjudicado individual podría activar una responsabilidad solidaria de la sociedad, como persona jurídica que asume los efectos perjudiciales que derivan para terceros de una actuación ilícita de sus administradores, que en este caso se le imputa además como responsable o encargada del tratamiento de datos, y de los administradores como causantes directos del daño cuya indemnización persigue la acción individual. Solventada la reparación del daño al tercero, se abrirá la posibilidad de ejercer derecho de regreso o repetición por quien corresponda, previsiblemente por la sociedad contra los administradores si fue ella quien indemnizó al perjudicado, lo que podrá hacer a través de la acción social, con esa finalidad y con la de repercutir la sanción administrativa que se le hubiera podido imponer como consecuencia de la infracción.

Finalmente, frente a esta vertiente de responsabilidad por daño al patrimonio social, cabe pensar en otras variantes de la relación entre el deber de diligencia y la disponibilidad y tratamiento de los datos. Por un lado, teniendo en cuenta que el deber de diligencia tiene una manifestación específica en el derecho/deber de información adecuada y necesaria para el desempeño del cargo, existirán situaciones, cada vez más frecuentes, en que la adopción de las decisiones más correctas, bien para desarrollar una determinada actuación, bien para modificarla, sustituirla o descartarla, especialmente si tiene carácter estratégico para el desarrollo del objeto social, exigirá acceder y utilizar razonablemente datos, a menudo ya "big data", al menos dentro de una disponibilidad proporcionada a las circunstancias concretas de la sociedad y del contexto en que la situación se plantea. Podrá entonces ocurrir que, por no obtener

disponibilidad de datos que era factible obtener, por no considerar o utilizar los disponibles, etc., puedan tomarse decisiones perjudiciales para la sociedad, o dejen de tomarse decisiones que debieran haberse tomado, produciéndose en un caso y en otro daños causalmente vinculados a tal conducta. Cabrá entonces apreciar infracción del deber de diligencia, en esa dimensión de actuar con la información adecuada y necesaria a la que se refiere el artículo 225 de la Ley de Sociedades de Capital.

Por su parte, también habrá de tenerse en cuenta que actuar con información suficiente es uno de los presupuestos básicos para que proceda la aplicación de la regla de protección de la discrecionalidad empresarial, hoy contemplada en el artículo 226, a la hora de adoptar decisiones estratégicas y de negocio, sujetas a la discrecionalidad empresarial. La finalidad implícita de la norma, que es la de entender cumplido el estándar de diligencia del ordenado empresario, despliega sus efectos de forma más relevante cuando pueda operar como causa de exoneración de los eventuales perjuicios que puedan derivar de tales decisiones, si están cubiertas por la regla de protección. Cabrá igualmente entender en determinadas situaciones concretas que tal presupuesto de "información suficiente" para que la decisión estratégica o de negocio esté protegida implicará la utilización de datos, disponibles o de disponibilidad factible, que objetivamente contribuyan a la decisión más correcta o sin los cuales no hay garantía razonable de adoptar la decisión más correcta. Esta particular aplicación del deber de diligencia, aquí relacionado con el tratamiento y utilización de datos para la toma de decisiones correctas, supondrá entonces una nueva manifestación complementaria de la principalmente examinada a propósito del cumplimiento o incumplimiento de las obligaciones legales, pero con incidencia igualmente relevante, tanto en el contenido del deber, como en la exigencia de responsabilidad por su infracción o en la invocación efectiva de una causa de exoneración si derivan daños de una decisión empresarial sometida a riesgo pero protegida como decisión discrecional.