

N/REF: 0025/2025

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del mismo que va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que se acaban de señalar, se valora positivamente la referencia incluida tanto en la Memoria de Análisis de Impacto Normativo, como en su Exposición inicial previa al articulado, indicándose que: *Se ha recabado informe de la Secretaría General Técnica del Departamento y de la Agencia Española de Protección de Datos.*

I

El proyecto de Orden que se informa tiene por objeto la aprobación de la Política de Seguridad de la Información (PSI) en el ámbito del Ministerio de Industria y Turismo, lo que incluye la creación de los órganos de gobierno de la seguridad de la información y la regulación de las competencias asignadas.

A través de esta Orden se persigue el objetivo de dar estricto cumplimiento a varios artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en especial al artículo 12.3, por el que se dispone que: *En la Administración General del Estado, cada Ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.*

Asimismo, este proyecto de Orden Ministerial se estructura en un preámbulo, diecinueve artículos, una disposición adicional, una disposición derogatoria única y una disposición final única.

Además, tal y como se ha transcrito ut supra el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad —ENS— en su artículo 12.3, prevé que *“En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento”*, disponiéndose en el apartado 6 del propio artículo 12, que la política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los requisitos mínimos que en dicho Esquema Nacional se contemplan. Todo ello, con especial atención en garantizar el debido cumplimiento de lo dispuesto en la normativa de protección de datos.

II

En relación, precisamente, con lo que atañe a la protección de datos de carácter personal, este proyecto de Orden Ministerial contiene numerosas referencias. A modo de ejemplo, cabe citar el artículo 2 sobre marco normativo, el cual contiene la sujeción al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantías de los derechos digitales; el artículo 3 sobre principios de la seguridad de la información, el cual contempla en su inciso primero como uno de ellos la: *Seguridad desde el diseño y por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto, debiendo tener en cuenta la protección de datos personales y de la información clasificada en los supuestos en que aplique*; añadiendo, en su inciso segundo en materia de principios particulares y responsabilidades específicas que: *Protección de datos personales: se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. Tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser apropiadas en función del análisis de riesgos, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas*. El artículo 4 sobre estructura organizativa, por el que se regulan las personas designadas como Delegado de Protección de Datos y Delegados de Protección de Datos de los organismos públicos adscritos al Departamento; o el artículo 15.3 por el que se establece que: *“Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y, en especial, las guías elaboradas por el Centro Criptológico Nacional, y la Agencia Española de Protección de Datos, y el artículo 14 del Real Decreto 311/2022, de 3 de Mayo”*.

Por su parte, la figura del delegado de protección de datos se regula pormenorizadamente en el artículo 11 y la cláusula general en materia de protección de datos se regula en el artículo 17. En primero de los citados determina que:

“ 1. En el ámbito del tratamiento de datos personales, y sin perjuicio de las atribuciones establecidas en el RGPD de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de los Responsables de la Seguridad, el Delegado de Protección de Datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma.

2. El Delegado de Protección de Datos prestará asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto, serán responsabilidad de los respectivos responsables del tratamiento.

3. Ejercerá labores de asistencia y asesoramiento a los responsables del tratamiento de datos personales, a los Responsables de la Seguridad y a los responsables del Sistema, en los procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad de la información.

4. Prestará asesoramiento a los Responsables de la Seguridad y a los Responsables del Sistema, en cuanto a la implantación de medidas de seguridad de la información que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo”.

En segundo de los citados, en cuanto a régimen de protección de datos de carácter personal el citado artículo 17 establece que:

“Todos los sistemas de información del Departamento se ajustarán a las medidas de seguridad derivadas de los análisis de riesgos de los tratamientos de datos personales, así como de la evaluación de impacto relativa a la protección de datos en los términos recogidos por la normativa de protección de datos de personales. En caso de conflicto con la normativa de seguridad de la información indicada en el artículo 14 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos personales, según el criterio del Delegado de Protección de Datos”.

Centrándonos en el análisis del contenido de este precepto, se observa que se limita a establecer la obligación general de sujeción a las medidas de seguridad derivadas: i) del análisis de riesgos de los tratamientos en materia de datos personales, y ii) de elaborar la evaluación de impacto en los términos previstos en la normativa específica; y a disponer que, en caso de conflicto, prevalecerá la normativa que presente un mayor nivel de exigencia respecto de la protección de datos, según el criterio establecido por el Delegado de Protección de Datos.

La parquedad de su regulación provoca que dicho artículo 17 no contenga regulación alguna sobre la figura del Delegado de Protección de Datos, carencia que, sin embargo, resulta compensada y coherente con la organización sistemática de esta Orden, dado que con carácter previo a la cláusula en materia de protección de datos personales en el artículo 11 regula de manera amplia y pormenorizada la figura del Delegado de Protección de Datos, en similares términos que los dispuestos en la Sección 4 del Capítulo IV del Reglamento General de Protección de Datos y en el Capítulo III del Título V de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Dicho Delegado de Protección de Datos deberá ejercer las labores de asesoramiento y supervisión en el ámbito de la Orden que se informa, prestando asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a su puesta en práctica.

A su vez, debe reiterarse que, de acuerdo con la regulación general del artículo 37 del RGPD y del artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, la designación del Delegado debe efectuarse de conformidad con lo dispuesto por la legislación aplicable en materia de protección de datos. En consecuencia, dicho delegado deberá ser nombrado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos, y a su capacidad para desempeñar las funciones que tiene encomendadas.

Ahora bien, además de la figura del Delegado de Protección de Datos cuya ausencia de regulación en este artículo se encuentra compensada con la regulación contenida en el artículo 11, se advierte, sin embargo, la ausencia de regulación expresa de determinadas cuestiones que sí sería conveniente incorporar a su contenido.

La primera de ellas sería la relativa a incorporar la sujeción en todos los tratamientos a los principios generales y esenciales en materia de datos personales previstos en el artículo 5 RGPD, sin cuyo respeto sería imposible apreciar la validez del tratamiento.

La segunda cuestión se refiere a la conveniencia de incorporar la precisión semántica de referirse a medidas “técnicas y organizativas” siguiendo la propia terminología empleada por el legislador. En este sentido, cuando se regula el tratamiento de datos de carácter personal, y se prevé el pleno sometimiento de los tratamientos de datos realizados, a las medidas de seguridad reguladas en la normativa de protección de datos personales, se debe añadir la referencia a tratarse de “medidas técnicas u organizativas”

En tercer lugar, se advierte la conveniencia de enfatizar o destacar la posible adopción de medidas agravadas respecto a las que, además, hayan de aplicarse conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Así, sería conveniente precisar en este precepto que las medidas de seguridad que resulten apropiadas en cada caso, y derivadas del análisis de riesgos, así como de la realización de una evaluación de impacto relativa a la protección de datos, según se detalla en el RGPD y en la LOPDGDD, podrán concretarse en determinadas **medidas agravadas** respecto a las que, además, hayan de aplicarse conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En consecuencia, sin perjuicio de ser conforme a Derecho la actual redacción propuesta se aconseja su revisión con el fin de ampliarla, garantizando que contenga referencia expresa a todas las cuestiones relacionadas con la realización de los tratamientos de datos derivados de lo establecido en la propia Orden con sujeción a la normativa vigente.

En síntesis, se sugiere que el contenido del artículo 17 haga referencia expresa a las siguientes cuestiones:

- i) Sujeción en todos los tratamientos a los principios generales y esenciales en materia de datos personales.
- ii) Obligación general de sujeción a las medidas de seguridad “técnicas y organizativas” derivadas del análisis de riesgos de los tratamientos en materia de datos personales, y obligación general de elaborar la evaluación de impacto en los términos previstos en la normativa específica.
- iii) Prevalencia de la normativa que presente un mayor nivel de exigencia respecto de la protección de datos, según el criterio establecido por el Delegado de Protección de Datos, en caso de conflicto con la normativa de seguridad de la información indicada en el artículo 14.
- iv) Referencia expresa a la necesidad de adoptar las medidas agravadas que resulten del análisis de riesgos respecto de la normativa contenida en Real Decreto 311/2022, de 3 de mayo.

A tal fin, se propone por esta Agencia sustituir la redacción actual del artículo 17 sobre protección de datos de carácter personal por la siguiente redacción o similar:

1. *El tratamiento de datos de carácter personal en el ámbito del Ministerio de Industria y Turismo se efectuará conforme a los principios de licitud, transparencia y lealtad, finalidad, minimización, exactitud, limitación del plazo de conservación, integridad y confidencialidad, así como responsabilidad proactiva y seguridad.*
2. *Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de los órganos superiores y directivos del Ministerio de Industria y*

Turismo, además de sus organismos y entidades adscritas o dependientes, ya sean tratamientos automatizados o no automatizados, las medidas de seguridad técnicas y organizativas apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos personales, conforme se detalla en 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 (Reglamento general de protección de datos).

- 3. En caso de conflicto con la normativa de seguridad de la información indicada en el artículo 14 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos personales, según el criterio del Delegado de Protección de Datos.*
- 4. Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad correspondientes a la categoría del Sistema según el anexo II del Real Decreto 311/2022, de 3 de enero, por el que se regula el Esquema Nacional de Seguridad. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.*

III

La normativa de protección de datos plantea nuevos retos, entre los que destaca la necesidad de ofrecer un nuevo enfoque al tratamiento de datos de carácter personal. De este modo, para garantizar su adecuada implantación resulta necesario intensificar la labor de coordinación con el resto de las normas de implantación obligatoria en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas regulaciones. Dichas normas se enumeran de forma detallada en el artículo dos de esta Orden Ministerial, relativo al marco normativo, desarrollándose su contenido en los principios de la seguridad de la información de su artículo tercero.

Asimismo, el artículo 3, letra d) establece, dentro de los principios básicos de la seguridad de la información —siguiendo en este punto lo dispuesto en los artículos 5. b), 7 y 10 del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo) — el de “Gestión de los riesgos”, que será parte esencial del proceso de seguridad, estableciendo que: *de acuerdo con lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 7 del Real Decreto 311/2022, de 3 de mayo, el análisis y gestión de riesgos será parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales y de los datos de material clasificado según la normativa sobre secretos oficiales.*

A su vez, el artículo 3.1. letra g), dentro de dichas directrices fundamentales de seguridad, que deben orientar la actuación del Departamento, señala la adopción del principio de “Seguridad desde el diseño y por defecto”, en los siguientes términos: *los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto, debiendo tener en cuenta la protección de datos personales y de la información clasificada en los supuestos en que aplique.*

Pues bien, la citada regulación —que supone una remisión expresa a la normativa de protección de datos en cuanto a la adopción de las correspondientes medidas de seguridad técnicas y organizativas—, resulta **plenamente conforme con la normativa de protección de datos, por lo que se informa favorablemente el contenido de dichos artículos.**

IV

En cuanto a la **gestión de la seguridad en el Ministerio**, se establece en el artículo cuarto el desarrollo de su estructura organizativa en relación con la seguridad de la información, incluyendo los principales órganos y figuras responsables de su implantación y seguimiento. Entre ellos, destacan la Comisión Ministerial de Administración Digital (CMAD) y el Grupo Técnico de Seguridad de la Información (GTSI), así como los Responsables de Seguridad (RSeg), de Sistemas (RInf), Personas designadas como Delegados de Protección de Datos, Personas designadas como Administradores de Seguridad, Jefes de Seguridad de Órganos de Control de los Servicios de Protección de la Información Clasificada, Célula Ministerial de Crisis, y el Servicio Central de Protección de la Información y el Subregistro Principal OTAN/UE. Todos ellos desempeñan funciones específicas en el marco de la Política de Seguridad de la Información para garantizar su correcta aplicación, mantenimiento y evolución, lo cual se informa asimismo favorablemente.

En cuanto al **Delegado de Protección de Datos —DPD—**, como se ha mencionado con anterioridad su naturaleza y funciones se regulan en el artículo 11 del proyecto de Orden, correspondiéndole prestar asistencia y asesoramiento a los responsables del tratamiento, a los responsables de seguridad y a los responsables de sistemas, en los procesos de gestión de brechas de datos personales, y en cuanto a la implantación de medidas de seguridad de la información que tengan un objeto distinto que la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.

Según se expuso anteriormente, la designación del Delegado en el Ministerio y organismos adheridos deberá basarse en su cualificación profesional, experiencia y conocimientos jurídicos, debiendo ser nombrados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos, y a su capacidad para desempeñar las funciones que tienen encomendadas.

A este respecto, teniendo en cuenta la regulación general de la figura del Delegado —cuyas funciones se contienen en la Sección 4 del Capítulo IV del Reglamento General de Protección de Datos y en el Capítulo III del Título V de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales—, **las previsiones del artículo 11 del proyecto de Orden, resultan conformes con la normativa de protección de datos, si bien ha de reiterarse que la designación del delegado debe efectuarse de conformidad con lo dispuesto por la legislación aplicable en materia de protección de datos, especialmente en atención a la regulación del artículo 37 del RGPD y del artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre.**

V

Por lo demás, según se advierte, el texto que se informa considera la evolución de las políticas de seguridad de la información desde un modelo de lista de cumplimiento a otro de **análisis de riesgo y de impacto en la protección de datos (responsabilidad proactiva, art. 5.2 RGPD)**, quedando dicho enfoque claramente plasmado en el texto que se informa, con estricta observancia de los artículos 24 y 32.1 del RGPD, y en consonancia con las previsiones de su Considerando 75.

La determinación de las diferentes funciones asignadas a los distintos agentes en materia de seguridad previstas en los artículos 5 y siguientes, con especial mención al artículo 11 sobre delegado de protección de datos, resultan pormenorizadas y adecuadas. **Debiendo hacerse especial mención a la diferenciación de responsabilidades tal y como señala expresamente el artículo 8.5:** *La personas designadas Responsable de la Seguridad no podrán ser designadas como Responsable de la Información, ni de los Servicios. Adicionalmente, deberán ser distintas del Responsable de los Sistemas y no podrá existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que el Responsable de la Seguridad y el Responsable de los Sistemas recaiga en la misma persona, o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo.*

En relación con esta cuestión de diferenciación de responsabilidades, tal y como ya se ha analizado en este informe, las medidas a implantar como consecuencia del análisis de riesgos previsto en el artículo 32 del RGPD, **en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre éstas últimas**, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos. Debiendo hacerse notar a este respecto la conveniencia de deslindar claramente los ámbitos funcionales del Responsable de Seguridad del Esquema Nacional de Seguridad y del Delegado de Protección de Datos como una de las posibles medidas agravadas adoptadas a consecuencia del análisis de riesgos, tal y como se indicó en nuestro citado **Informe 170/2018, de 12 de noviembre de 2018**, en el que se analizó la diferenciación entre la figura del Delegado de Protección de Datos y el Responsable de Seguridad; informe que, por su interés en el presente caso, reproducimos parcialmente a continuación:

“Con carácter previo a analizar la concreta cuestión planteada en la consulta, este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan.

En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados “Tecnologías de la Información y las Comunicaciones -TIC-”), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, cuyo Preámbulo señala que “la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios” añadiendo que “en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles”.

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual “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”. Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 “no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos”.

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

“La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso 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». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho 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 respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva”.

Y en este mismo sentido se pronuncia 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que tiene por objeto “proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales” (artículo 1.2.), destacando en su Considerando 1 que “la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental” y en su Considerando 10 que “para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo”.

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento” y “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para “asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento” (artículo 57.1.c) RGPD)”.

Conclusiones

Primera. El proyecto de Orden analizado cumple con las exigencias en materia de protección de datos personales, al prever expresamente el pleno sometimiento a su normativa, la realización del correspondiente análisis de riesgos y, en su caso, de la evaluación de impacto, en aquellos sistemas que traten datos personales, conforme al RGPD y a la LOPDGDD. Todas estas previsiones resultan de su articulado, pero no todas ellas se contienen expresamente en el artículo 17 en materia de protección de datos, proponiéndose una nueva redacción de este precepto a fin de introducir referencia expresa en el mismo: i) al debido respeto al conjunto de principios relativos al tratamiento del artículo 5 RGPD, ii) a las medidas de seguridad “técnicas y organizativas”, iii) a la adopción de las medidas agravadas que resulten del análisis de riesgos respecto de la normativa contenida en el Real Decreto 311/2022, de 3 de mayo.

Segunda. Por lo demás, el articulado de este proyecto de Orden desarrolla detalladamente la metodología de gestión de seguridad y de riesgos, y la asignación de responsabilidades, asegurando la prevalencia de la normativa de protección de datos en todo el proceso. Con especial mención a la diferenciación de responsabilidades, y a la distinción de las figuras del Delegado de Protección de Datos y del Responsable de Seguridad, tal y como se explica en nuestro informe 170/2018.