

N/REF: 0024/2024

I

La consulta plantea el análisis de la Orden de referencia la cual tiene por objeto de conformidad con lo previsto en su artículo 1: *“(....) regular los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos del Organismo Estatal Inspección de Trabajo y Seguridad Social, así como la adopción de medidas de cooperación por parte de las autoridades competentes que intervienen en el procedimiento sancionador en el orden social para facilitar a las personas interesadas la realización de trámites a través de representante.*

Todo ello de conformidad con lo previsto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; en el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo; en el Reglamento general sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatorios de cuotas de la Seguridad Social, aprobado por Real Decreto 928/1998, de 14 de mayo; y en el Reglamento de organización y funcionamiento de la Inspección de Trabajo y Seguridad Social, aprobado por Real Decreto 138/2000, de 4 de febrero”.

El proyecto consta de un preámbulo, 19 artículos (estructurados en tres capítulos), tres disposiciones adicionales, una disposición transitoria y tres disposiciones finales, junto con cinco anexos. Asimismo, no deroga expresamente ninguna norma.

II

Entrando al análisis de su contenido desde el punto de vista de la protección de datos de carácter personal procede comenzar indicando que los datos personales constituyen la materia prima de la sociedad de la información, algunos autores los califican como el petróleo de la economía digital, de manera que difícilmente los servicios públicos y la sociedad del bienestar o las empresas podrán funcionar actualmente de una manera adecuada sin ellos.

Dado su reconocimiento como un derecho fundamental, estos datos personales (que son en realidad cualquier dato o información de una persona física identificada o identificable) no pueden utilizarse sin más, sino que deben

respetarse unas reglas sobre su utilización, las cuales indican cuándo y cómo pueden ser tratados.

En el ámbito internacional, las primeras iniciativas surgieron en el marco del Consejo de Europa, así la Resolución 1968 sentó las bases de unos principios que regulaban el tratamiento de la información de datos personales. A partir de entonces se ha ido sucediendo la producción de normas en los ámbitos internacional, europeo, nacional y autonómico. En este contexto las principales normas, a día de hoy son, en síntesis:

1. Reglamento general de protección de DP UE 2016/679 del Parlamento y del Consejo, 27 de abril de 2016.
2. Directiva 2016/680, relativa al tratamiento para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.
3. LO 3/1018, de 5 de diciembre, de protección de DP y garantías de los derechos digitales, y que sustituye a la anterior LOPDCP de 1999, esta LO adapta al marco español el Reglamento europeo y desarrolla algunos de sus aspectos.

Las citadas normas establecen el marco normativo básico en materia de protección de datos que luego se podrá concretar en cada sector específico.

El proyecto normativo objeto de esta consulta en lo relativo al régimen jurídico de datos personales proyecta su regulación en el artículo 3 con el siguiente tenor literal:

1. La titularidad y gestión de la aplicación informática de apoderamientos que se regula en esta orden corresponde al Organismo Estatal Inspección de Trabajo y Seguridad Social, por lo que al mismo le corresponde la condición de responsable del tratamiento de datos personales. Por su parte, corresponden a la Unidad de Tecnologías de la Información, Comunicaciones y Apoyo a la Planificación del Organismo las funciones de encargado de dicho tratamiento.

2. De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona poderdante o la persona apoderada fueran personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento de la aplicación informática de apoderamientos se fundamenta en la letra e) del artículo 6.1. del RGPD, en relación con los artículos 5 y 6 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, sin perjuicio de que sea necesaria la adopción de las medidas técnicas y organizativas a las que se refiere el apartado 5.

En todo caso, el tratamiento de datos personales que supone la aplicación de la presente orden se registrará por el principio de protección de los datos personales, derivado del previo análisis de los riesgos y evaluación de impacto de los derechos y libertades físicas, que serán revisadas y actualizadas cuando sea necesario.

3. Como garantía del principio de limitación de la finalidad, los datos personales recogidos en la aplicación no podrán tratarse para una finalidad diferente a la acreditación de la existencia y vigencia de un apoderamiento inscrito.

4. Se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales y que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad prevalecerán sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el RGPD”.

A la vista de la anterior previsión normativa se aprecia la ausencia de una referencia expresa, previa y genérica a la normativa en materia de protección de datos respecto de todos los tratamientos de datos personales que pudieran llegar a realizarse a través del proyectado Registro Electrónico de Apoderamientos. Así, a pesar de que se contempla la sujeción a una de las bases jurídicas del artículo 6 RGPD y la adopción de medidas técnicas y organizativas de acuerdo con el artículo 5 RGPD, se aconseja la inclusión de una cláusula de salvaguarda general que garantice el necesario respecto de esta normativa en todos los tratamientos de datos personales que pudieran llevarse a cabo al amparo de esta Orden. Igualmente, se aconseja su inclusión al inicio de este artículo y se propone como sugerencia el siguiente texto normativo:

“Todos tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el 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 en el resto de la normativa sobre protección de datos personales”.

III

En siguiente lugar, entrando al análisis del párrafo segundo del artículo 6 conviene comenzar enfatizando la necesidad de que, en efecto, todo tratamiento de datos personales se fundamente no solo en una de las bases legitimadoras del artículo 6, al no ser el nuestro un sistema voluntarista, y ser solo posible en alguno de los supuestos legalmente permitidos; sino también en la necesidad de que garantice el respeto de todos y cada uno de los principios relativos al tratamiento previstos en el artículo 5 inmediatamente anterior. Dichos principios representan una consolidación de los que tradicionalmente han venido siendo utilizados a propósito de estos tratamientos, y constituyen

las líneas maestras de cómo han de realizarse aquéllos, sin perjuicio de destacar el cambio de paradigma que ha supuesto la inclusión como piedra angular del sistema a partir de 2016 del principio de responsabilidad proactiva. En síntesis, el citado artículo 5 recoge expresa referencia a los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; integridad y confidencialidad; limitación del plazo de conservación; y responsabilidad proactiva.

El respeto de todos ellos junto con la indispensable existencia de una de las bases legitimadoras previstas en el artículo 6 RGPD constituye una *conditio sine qua non* de licitud inicial de todo tratamiento de datos personales. A este respecto, la redacción actualmente prevista del segundo párrafo in fine del proyecto normativo objeto de esta consulta dispone que:

“(...) En todo caso, el tratamiento de datos personales que supone la aplicación de la presente orden se registrará por el principio de protección de los datos personales, derivado del previo análisis de los riesgos y evaluación de impacto de los derechos y libertades físicas, que serán revisadas y actualizadas cuando sea necesario”. A la vista de que la redacción proyectada contiene una referencia un tanto imprecisa al principio de protección de datos personales se recomienda su revisión para ceñirse en la medida de lo posible a alguno de los principios específicamente regulados en el RGPD, sin perjuicio de enfatizar el necesario respeto de todos ellos.

Centrándonos por otra parte en el análisis de la base legitimadora prevista en el artículo 3, segundo párrafo de la norma proyectada, con remisión al artículo 6.e) RGPD en cuya virtud se dispone que: *“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: (...) e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; (...)”*, proceder señalar la necesidad de atender al mismo tiempo a la redacción prevista en el artículo 8.2 de la LO 3/2018, de 5 de diciembre: *“2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley”.*

En este sentido, cabe destacar que la actual redacción del citado artículo 3 en su párrafo segundo vincula la elección de la base legitimadora de referencia a los artículos 5 y 6 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, que regulan respectivamente la representación y los registros electrónicos de apoderamientos, estableciendo el artículo 6.1 que: *“La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales dispondrán de un registro electrónico general de apoderamientos, en el que deberán*

inscribirse, al menos, los de carácter general otorgados apud acta, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo a favor de representante, para actuar en su nombre ante las Administraciones Públicas. También deberá constar el bastanteo realizado del poder.

En el ámbito estatal, este registro será el Registro Electrónico de Apoderamientos de la Administración General del Estado.

Los registros generales de apoderamientos no impedirán la existencia de registros particulares en cada Organismo donde se inscriban los poderes otorgados para la realización de trámites específicos en el mismo. Cada Organismo podrá disponer de su propio registro electrónico de apoderamientos”.

Por lo expuesto, se observa la efectiva referencia a una norma legal que atribuye esta competencia en materia de registros electrónicos de apoderamientos a los Organismos Públicos.

En cuanto a la extensión de la expresión del art. 6.1.e) RGPD como base jurídica del tratamiento de datos personales, cabría plantearse si “todo tratamiento de datos personales por una Administración pública estaría en todo caso amparado por la letra e)”, y ante tal cuestión la respuesta ha de ser necesariamente negativa, puesto que el art. 6.1.e) RGPD tan sólo considera lícito un tratamiento de datos personales sobre la base de dicho precepto si el mismo es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, en virtud de una competencia atribuida por una norma con rango de ley. Por ello, si un determinado tratamiento no es “necesario” para el cumplimiento de la misión realizada en interés público o en el ejercicio de los poderes públicos conferidos por el ordenamiento, dicho tratamiento no sólo carecería de base jurídica suficiente legitimadora prevista en el apartado e), sino que, además, infringiría el principio de minimización de datos contenido en el artículo 5.1.c) RGPD, aplicable igualmente a los tratamientos de datos llevados a cabo por la Administración pública.

En esta misma línea, resulta oportuno recordar que la Administración está vinculada al principio de legalidad, de manera que, a diferencia de los particulares, tan sólo puede llevar a cabo aquello que el ordenamiento jurídico le permite expresamente. Este es el sentido de lo dispuesto en los artículos 9.1 y 103 de la Constitución, de suerte que cuando la ley y el derecho no han atribuido a la Administración las potestades correspondientes para actuar ante una determinada situación, esa actuación no podrá llevarse a cabo sin que previamente el ordenamiento le atribuya dichas potestades. No existe, por tanto, un espacio vacío donde a falta de ley pueda la Administración actuar. Es

lo que se ha denominado la doctrina de la “vinculación positiva de la Administración a la legalidad” (García de Enterría). En consecuencia, para que la Administración pueda actuar necesita de una previa habilitación legal (entendida aquí legalidad como habilitación normativa). Y ello tanto si la Administración actúa en el ámbito del derecho público como el ámbito del derecho privado. Así podemos ver que incluso en este último ámbito, en el que actuaría en el mismo rango que los particulares, la Administración necesita una norma que le habilite a actuar. Como ejemplo cabe citar que el Estado puede ser heredero (ejemplo de actuación en derecho privado), bien testamentario bien abintestato (art. 20 de la ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas). Como tal heredero tiene la misma posición que los demás llamados a la sucesión, pero la posibilidad de aceptar la herencia se regula en dicha ley, por lo que en todo caso la aceptación habrá de hacerse a beneficio de inventario (art. 20.1). Los tratamientos de datos que necesite realizar la Administración para tal fin tendrían, en principio, como base jurídica legitimadora la propia base establecida en el artículo 6.1.e) RGPD, esto es, que el tratamiento ha de ser necesario para cumplimiento de la misión realizada en interés público, por cuanto la Administración no sólo está vinculada positivamente a la ley y al derecho de manera que no puede actuar sin éste o a espaldas de este, sino que por ese mismo motivo toda su actuación esta guiada, en términos amplios, por el interés público, aunque su actuación se desenvuelva en el ámbito del derecho privado.

En cualquier caso, el RGPD excluye de la posibilidad de que los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones (sin distinguir si dichas funciones están sometidas al derecho público o al privado) puedan tener como base jurídica del tratamiento la letra f) del art. 6.1 RGPD, esto es, el interés legítimo. Ello, sin duda, porque parte de la base, como demuestra el considerando 45 RGPD, de que cuando se realice un tratamiento de datos en cumplimiento de una obligación legal aplicable al responsable del tratamiento o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, dicho tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. En definitiva, dicho tratamiento de datos estará amparado por la letra e) del art. 6.1 si el derecho aplicable ha atribuido una competencia a la Administración, y no lo estará en caso contrario. Obviamente, dichas potestades pueden desembocar en bases jurídicas específicas; así, por ejemplo, nadie discute que la Administración puede entrar en contratos, bien de derecho público o de derecho privado. En ambos casos dicha potestad de contratar ha de venir establecida por ley, en cuanto que regula la competencia y las facultades del órgano para contratar, pero nada impide que en estos casos el tratamiento pueda basarse en una base jurídica distinta, como es la del art. 6.1.b) RGPD, esto es, que el tratamiento sea necesario para la ejecución de un contrato, por cuanto el art. 6.1, primer inciso, establece que será suficiente para un tratamiento de datos lícito el que concurra al menos una (luego puede haber más de una) de las condiciones que el precepto regula.

IV

Finalmente, proceder a abordar el estudio del Análisis de riesgos y evaluación de impacto en materia de protección de datos recogido en el epígrafe 8 del punto IV, de Análisis Jurídico, de la Memoria de Análisis de Impacto Normativo Abreviada. Bajo este epígrafe se aprecia la elaboración de un análisis de riesgos de seguridad para los sistemas de información siguiendo el ENS cuyo examen excede de los límites de este informe, si bien se aprecia la ausencia de un análisis de riesgos y evaluación de impacto en materia de protección de datos propiamente dicho. Asimismo, tampoco se aprecia un análisis de riesgos para los derechos fundamentales de las personas con ocasión de estos tratamientos, ni una evaluación de impacto en materia de protección de datos.

A estos efectos, se recuerda la existencia de una Guía elaborada desde esta AEPD titulada “Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo” la cual tiene por finalidad servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de una Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas que sean competencia de la AEPD impliquen un tratamiento de datos personales.