N/REF: 0006/2021

Antes de entrar a analizar el texto sometido a informe, es preciso señalar que el mismo se emite sin que se haya aprobado el Real Decreto por el que se desarrollan la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, en materia de actuación y funcionamiento del sector público por medios electrónicos, encontrándose el correspondiente proyecto, tal y como se indica en la consulta, pendiente del preceptivo dictamen del Consejo de Estado. No obstante, teniendo en cuenta lo manifestado en la consulta y que, de acuerdo con la disposición final séptima de la Ley 39/2015, "las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico producirán efectos a partir del día 2 de abril de 2021", se procede a la emisión del mismo, sin perjuicio de que, si como consecuencia de las observaciones del alto órgano consultivo se introdujeran modificaciones en el proyecto que afecten sustancialmente al contenido de la presente Orden, debería solicitarse nuevo informe de esta Agencia.

El proyecto de orden objeto de informe tiene por objeto regular presente orden tiene por objeto regular el funcionamiento del Registro de funcionarios habilitados para la expedición de copias auténticas y para la identificación o firma electrónica de los interesados, previsto en los artículos 12 y 27 de la Ley 39/2015 y creado por el artículo 31 del proyecto de real decreto de desarrollo.

I

Esta Agencia ha tenido oportunidad de pronunciarse, en relación con la necesaria salvaguardia del derecho fundamental a la protección de datos personales en la Administración electrónica, en sus informes 26/2015 y 91/2018.

En el informe 26/2015, referente al Anteproyecto de Ley del Procedimiento Administrativo Común de las Administraciones Públicas ya destacó la necesidad de incluir expresamente, dentro de los derechos de las

personas en sus relaciones con la Administración, el de protección de sus datos de carácter personal, y en particular, en relación con los registros electrónicos, a la necesidad de implantar en los mismos las medidas de seguridad previstas en la normativa de protección de datos, a fin de garantizar que no se produzca la pérdida, acceso accidental o destrucción de los documentos o solicitudes presentadas por los ciudadanos que pudieran contener datos de carácter personal, señalando que

> Particularmente relevante será la referencia a la necesaria adopción de las medidas de seguridad establecidas no sólo en el Esquema Nacional de Seguridad sino también la normativa de protección de datos de carácter personal dentro de la normativa reguladora de los registros a los que se refiere el Anteproyecto y, en particular, en el Registro de apoderamientos y en los regulados por el artículo 30.

Posteriormente, el informe 91/2018 referente al proyecto de Real Decreto por el que se desarrollan las leyes 39/2015 y 40/2015 ambas de 1 de octubre de 2015, en materia de actuación y funcionamiento del sector público por medios electrónicos, incidía en la necesidad de garantizar, en dichas normas de desarrollo, el derecho a la protección de datos de carácter personal, tal y como se había recogido en la Ley 39/2015 tras las anteriores observaciones:

> La norma presentada a informe es, tal y como proclama su título, desarrollo de las leyes 39/2015 y 40/2015, de 1 de octubre (en adelante leyes 39/2015 y/o 40/2015) en materia de actuación y funcionamiento del sector público por medios electrónicos. Pues bien, una primera conclusión que cabe extraer, y que desde el punto de vista del informe de esta Agencia podría ser suficiente, es que dichas leyes contienen ya una referencia explícita a que las relaciones entre las Administraciones Públicas, o en las relaciones de estas con los interesados, habrá de cumplirse en todo momento con la normativa de protección de datos, circunstancia ésta, como no puede ser de otro modo, que se extiende igualmente a sus normas de desarrollo. Así, cabe mencionar que dichas obligaciones se recogen en los artículos 13.h), 16.1 (3º) y 17 de la ley 39/2015, y en los artículos 3.2, 4.2 y 155 de la ley 40/2015.
>
> El art. 13 h) de la ley 39/2015 establece como un derecho de las personas en sus relaciones con las administraciones públicas el de la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Ello se extiende a los registros, en cuanto que cauce esencial de las solicitudes de los administrados a las Administraciones: Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal. (art. 16.1 de la ley 39/2015), y también se extiende a los archivos, como soporte electrónico de los documentos de procedimientos finalizados: Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos. (art. 17.3º de la ley 39/2015).

Desde el punto de vista del régimen jurídico de las Administraciones Públicas, la ley 40/2015 establece como un principio general de su actuación y de las relaciones entre las mismas el de garantizar […] la protección de los datos de carácter personal, (de los ciudadanos que se relacionan con ella) –art. 3.2 ley 40/2015. Y el art. 4.2 de dicha norma reconoce el valor del derecho fundamental a la protección de datos personales como un límite a la actuación administrativa, lo que corrobora el art. 155, ya que las transmisiones de datos entre las Administraciones Públicas han de estar sujetas a lo permitido por la normativa de protección de datos personales.

En definitiva, la actuación y el funcionamiento del sector público por medios electrónicos conlleva una serie de ventajas en materia de eficacia, eficiencia, simplicidad, racionalización de costes etc. pero no podemos dejar de mencionar que también existen más riesgos para el derecho fundamental de los particulares a la protección de sus datos personales, por lo que las leyes 39/2015 y 40/2015 han hecho hincapié en que dichos medios electrónicos han de ser usados siempre de conformidad con la normativa de protección de datos. Y dicha normativa habrá de ser cumplida por lo tanto escrupulosamente cuando de las normas de desarrollo de dichas leyes se trata, o de las actuaciones específicas derivadas de las mismas, pues en caso contrario dichas normas de desarrollo o actuaciones que incumpliesen los mandatos de la ley estarían incursos en causas de invalidez (art. 47 y 48 ley 39/2015).

II

En lo que a la materia de protección de datos personales se refiere, la normativa a la que debe ajustarse la Orden proyectada está constituida por 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 por el que se deroga la Directiva 95/46/CE (RGPD en lo sucesivo) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo), que tiene incidencia en diversos aspectos regulados en la norma, que se analizarán siguiendo el orden de su articulado.

En primer lugar, el artículo 5 regula el Contenido del Registro de funcionarios habilitados:

> En el Registro constarán, al menos, los siguientes datos de los funcionarios habilitados:
> a) Documento nacional de identidad, NIE.
> b) Nombre y apellidos del funcionario.
> c) Órgano, organismo o entidad en el la que presta servicios el funcionario, centro directivo y centro de destino identificados mediante su código asignado en el Directorio Común de Unidades Orgánicas y Oficinas, indicándose el código de oficina para el caso de funcionarios destinados en una oficina de asistencia en materia de registros.
> d) Puesto de trabajo que desempeña.
> e) Correo electrónico
> f) Fecha de alta en el Registro de funcionarios habilitados.
> g) Tipo de habilitaciones: Identificación o firma electrónica y/o expedición de copias auténticas.
> h) Procedimientos y servicios para los que se tiene autorizada la habilitación, identificados mediante su código asignado en el Inventario de Información Administrativa.
> i) Fecha de baja en el Registro de funcionarios habilitados.
> j) Causas de las cancelaciones de las habilitaciones.

Por consiguiente, la Orden establece el contenido mínimo del Registro con un carácter abierto, ya que establece que dichos datos son los que se harán constar “al menos”, por lo que está admitiendo que se puedan incluir más datos en los formularios que pueda aprobar la Secretaría de Estado de Política Territorial y Función Pública, conforme a la disposición adicional única de la misma.

En este punto, hay que tener en cuenta, desde la perspectiva de la protección de datos personales, la vigencia del principio de minimización recogido en el artículo 5.1.c) del RPGD, de modo que los datos personales serán “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”. **Por ello, y tal y como se ha indicado para el**

Registro electrónico de apoderamientos en nuestro informe 4/2001, siendo la Orden informada la norma jurídica de inferior rango que regula los datos que deben figurar en el Registro, la enumeración contenida en la misma debería ser cerrada, especificando los datos que deben figurar en el mismo atendiendo al citado principio, sin dejar una puerta abierta a una mayor de desagregación de la información que podría incurrir, si se hiciera referencia a datos personales, a la infracción de ese mencionado principio de minimización si el dato no fuera indispensable para la finalidad del tratamiento.

Por otro lado, entre los datos que deben figurar en el Registro, se incluye el correspondiente al DNI o NIE del funcionario. A este respecto, conviene resaltar que el RGPD ha recogido la creciente preocupación sobre el tratamiento del número nacional de identificación, facultando a los Estados Miembros a regular las condiciones en las que se podrá proceder a dicho tratamiento y exigiendo la adopción de las garantías adecuados que salvaguarden la aplicación del reglamento, tal y como resulta de su artículo 87:

> Artículo 87 Tratamiento del número nacional de identificación.
>
> Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Precisamente, con la finalidad de introducir las necesarias garantías en el tratamiento del DNI por parte de las Administraciones Públicas, la LOPDGDD ha introducido una regulación específica al respecto en su disposición adicional séptima que, si bien referida al supuesto específico de notificaciones por medio de anuncios y publicaciones de actos administrativos, introduce garantías en el tratamiento del DNI de los interesados, partiendo de la base de la injerencia que puede suponer en el derecho fundamental a la protección de datos personales que se conozcan conjuntamente el nombre y apellidos y el DNI de una persona, además del importante riesgo de usurpación de identidad que puede producirse.

Por otro lado, siendo un Registro de funcionarios públicos, hay que tener en cuenta la existencia de otros identificadores de los mismos regulados en el Real Decreto 2073/1999, de 30 de diciembre, por el que se modifica el Reglamento del Registro Central de Personal y las normas de coordinación con los de las restantes Administraciones públicas, como el número de registro de personal o el número de identificación personal, que aún basados en el número del documento nacional de identidad, no se corresponden exactamente con el mismo.

Por todo ello, se considera que, atendiendo al principio de minimización de datos, debería valorarse la necesidad de que conste en el Registro el DNI o NIE del funcionario habilitado, teniendo en cuenta que el propio precepto ya se establecen otros datos que permiten la identificación del mismo. Y en el caso de que se considerara imprescindible una mayor identificación, debería valorarse la posibilidad de sustituirlos por el número de Identificación personal o el número de registro de personal.

III

El artículo 6 de la Orden regula los órganos competentes:

1. La Dirección General de Gobernanza Pública asume la gobernanza y gestión del Registro de funcionarios habilitados, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y 7 Transformación Digital el diseño, implantación, gestión técnica de la plataforma tecnológica que soporte el Registro.

2. El órgano que se determine por la Subsecretaría de cada ministerio o por el titular de cada organismo público será competente para la habilitación de los funcionarios que presten servicios en las unidades dependientes de los mismos, en base al modelo normalizado que se recoge como Anexo II. Dicho órgano será responsable de la inscripción, modificación y cancelación de los asientos registrales correspondientes a los funcionarios habilitados. Además, serán competentes para la habilitación de expedición de copias auténticas los órganos a los que se refiere el artículo 4.1 de esta Orden.

3. Producida la anotación de la habilitación del funcionario, el Registro generará una certificación en la que se hará constar la identificación personal y administrativa del funcionario, los procedimientos y servicios a los que alcanza su habilitación, la fecha de inicio de la misma y, en su caso, su fecha de fin, de acuerdo con el modelo del anexo II.

A este respecto se considera que, por razones sistemáticas y de coherencia con las Órdenes que van a regular el Registro electrónico de apoderamientos y el Registro electrónico general de la AGE, el citado precepto debería ir a continuación de la regulación del objeto y ámbito de aplicación de la Orden, como artículo 2.

Por otro lado, tal y como se ha señalado en nuestros informes 4/2021 y 5/2021, relativos a dichos Registros, desde la perspectiva de la normativa de protección de datos, es relevante identificar la posición jurídica que, en relación con los tratamientos de datos personales, corresponde a cada uno de dichos órganos, en función de su efectiva participación en la determinación de los fines y los medios el tratamiento. A este respecto, el RGPD considera en el artículo 4 como «responsable del tratamiento» o «responsable»: "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembro;" y como «encargado del tratamiento» o «encargado»: "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

En cuanto a la designación por el Derecho de los Estados miembros a que se refiere el artículo 4.7) del RGPD in fine ("si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembro"), las Directrices 07/2020 del Comité Europeo de Protección de Datos sobre los conceptos de responsable del tratamiento y encargado en el RGPD diferencia dos supuestos. Por un lado, los supuestos en los que el poder de decisión puede inferirse de una competencia legal explícita, por ejemplo, cuando el responsable del tratamiento o los criterios específicos para su nominación son designados por la legislación nacional o de la Unión. Cuando el responsable del tratamiento haya sido identificado específicamente por ley, esto será determinante para establecer quién actúa como responsable. Esto presupone que el legislador ha designado como responsable a la entidad que tiene una capacidad genuina para ejercer el control. Y que en algunos países, legislación nacional establece que las autoridades públicas son responsables del tratamiento de datos personales dentro del contexto de sus funciones (apartado 21). Y por otro, el supuesto más común en que, en lugar de nombrar directamente al responsable del tratamiento o establecer los criterios para su designación, la ley establece una tarea o impone un deber a alguien para captar y tratar ciertos datos. En esos casos, el fin del tratamiento a menudo está determinado por la ley y el responsable del tratamiento será normalmente el designado por ley para la realización de esta finalidad, como sería el caso cuando una entidad a la que se le confían determinadas tareas públicas (por ejemplo, seguridad social) que no puede cumplirse sin recopilar al menos algunos datos personales, establece una base de datos o registro para cumplir con esas tareas públicas. En ese caso, la ley, aunque indirectamente, establece quién es el responsable. De manera más general, la ley también puede imponer una obligación tanto a entidades públicas como privadas para retener o proporcionar ciertos datos. Estas entidades entonces normalmente se

considerarían como responsables con respecto al tratamiento que es necesario para ejecutar esta obligación (apartado 22).

Considerando que, en el presente caso, los fines y los medios del tratamiento han sido establecidos por la Ley 39/2015 y su reglamento de desarrollo, la concreción de dichas figuras vendrá determinada por las competencias que correspondan a cada uno de los órganos intervinientes y que se concretan en el precepto informado. **A este respecto, a la Dirección General de Gobernanza Pública le corresponde la "gobernanza y gestión" del Registro, por lo que a la misma le correspondería la condición de responsable del tratamiento. Mientras que la Secretaría General de Administración Digital asume el "diseño, implantación, gestión técnica de la plataforma tecnológica que soporte el Registro", por lo que estaría actuando como encargada del tratamiento.**

En cuanto al órgano competente para la habilitación de los funcionarios de los funcionarios que presten servicios en las unidades dependientes de cada Ministerio y organismo público, el mismo "será responsable de la inscripción, modificación y cancelación de los asientos registrales correspondientes a los funcionarios habilitados Además, serán competentes para la habilitación de expedición de copias auténticas los órganos a los que se refiere el artículo 4.1 de esta Orden".

A este respecto, hay que indicar que, a diferencia de las otras dos órdenes informadas, no se designa a dicho órgano como **Delegado del Registro, ni se establece el nivel orgánico que ha de tener el mismo, circunstancias que deberían revisarse para garantizar la debida homogeneidad en el funcionamiento de los Registros**. No obstante, se pueden reproducir nuestros argumentos en cuanto a que el mismo deberá actuar, en el ejercicio de dichas funciones, de acuerdo con las instrucciones que le pueda dar la Dirección General de Gobernanza Pública y no su superior orgánico, por lo que **en los tratamientos de datos personales que necesariamente ha de realizar para la inscripción, modificación y cancelación de los asientos registrales, estarán actuando por cuenta del responsable, como encargados del tratamiento**.

En relación con los encargados del tratamiento, deberá darse cumplimiento a lo dispuesto en el artículo 28 del RGPD, de modo que exista el acto o contrato que regule el citado encargo, en los términos señalados en el apartado 3 del citado precepto. A estos efectos, la propia Orden proyectada podrá ser dicho acto siempre que recoja los extremos que señala el citado artículo 28.3 del RGPD, lo que podría hacerse en un anexo de la misma.

Por último, en cuanto a la certificación a la que se refiere el apartado 3, debería especificarse en el precepto su finalidad y los destinatarios de la misma.

IV

El artículo 9 regula el acceso electrónico al Registro de Funcionarios Habilitados por las Administraciones Públicas.

> El Registro ofrecerá el acceso a la información sobre las habilitaciones por parte de los órganos de cualquier Administración Pública, así como de sus organismos públicos y entidades de derecho público.

Dicha regulación, en la que se ha suprimido cualquier referencia a la forma en la que se producirá el acceso, a diferencia de lo que se hacía en el artículo 8.2 de la Orden HAP/7/2014, de 8 de enero, por la que se regula el Registro de funcionarios habilitados para la identificación y autenticación de ciudadanos en el ámbito de la Administración General del Estado y sus organismos públicos vinculados o dependientes, es claramente insuficiente desde la perspectiva de la protección de datos personales. Por ello, debe modificarse el precepto, estableciendo la forma en la que se producirá el acceso, que deberá respetar los principio del RGPD, y establecer las garantías oportunas.

En este sentido, deberá tenerse en cuenta lo señalado en nuestro informe 4/2011 sobre el Registro electrónico de apoderamientos:

> El artículo 10 regula las consultas de los órganos y organismos públicos:
>
> El REA-AGE ofrecerá a los organismos interesados las siguientes vías de acceso a la información:
>
> b) Descarga, bajo petición, de un fichero, que contendrá todos los apoderamientos vigentes y válidos para los trámites y actuaciones por medios electrónicos de los que el órgano administrativo peticionario sea competente. El fichero contendrá todos los datos de los apoderamientos que se enumeran en el artículo 3 de esta Orden.
>
> b) Acceso en línea mediante servicios web, a los efectos de comprobar, automáticamente y en tiempo real desde las aplicaciones, que un apoderamiento está vigente. Las peticiones al REA-AGE, relativas a los apoderamientos vigentes y válidos para los procedimientos y trámites por medios electrónicos de las que el órgano administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello

electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte al Registro mantendrá trazabilidad de todas las peticiones recibidas.

Dicho precepto mantiene las dos posibilidades de acceso previstas en el artículo 11 de la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos. No obstante, esta Agencia considera que, de acuerdo con los principios recogidos en el artículo 5 del RGPD, el mantenimiento de ambas posibilidades resulta excesivo e incrementa los riesgos derivados del tratamiento de datos personales.

En primer lugar, la descarga del fichero procede solo en los casos en los que así se solicite, por lo que en otro caso debería acudirse al acceso en línea previsto en la letra b). Además, no se establece la periodicidad con la que debe realizarse dicha descarga, los que plantea el problema de dar cumplimiento al principio de exactitud de los datos previsto en la letra d) del artículo 5.1. del RGPD, de acuerdo con el cual los datos personales serán “exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan”. Por ello, pese a la descarga del archivo, y salvo que la misma se realizara de una manera prácticamente constante a fin de acreditar la vigencia de los poderes o las posibles rectificaciones realizadas en los datos de carácter personal, seguiría siendo necesario acudir al acceso en línea, para el cual, además, se han previsto unas garantías adicionales que no se establecen en el supuesto de descarga del fichero.

Por otro lado, la descarga del fichero va a permitir a los órganos y organismos de la Administración General del Estado y de otras administraciones que se adhieran al mismo acceder a todos los datos personales obrantes en el fichero, en la medida en que se refieran a trámites y actuaciones por medios electrónicos de los que el órgano administrativo peticionario sea competente, independientemente de que se correspondan con la tramitación de un procedimiento concreto, lo que sería excesivo y contrario al principio de minimización de datos, así como a la doctrina establecida por el Tribunal Constitucional contraria a los accesos masivos e indiscriminados a datos personales, recogida, entre otras, en su sentencia del Tribunal Constitucional17/2013, de 31 de enero.

Por todo ello, la descarga del fichero supondría un acceso masivo a datos personales que, además, no excluye la necesidad de acudir al acceso en línea para verificar la vigencia del poder siendo, por tanto,

contraria al principio de minimización de datos y al principio de proporcionalidad, en la medida en que exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad, recogido, entre otras, en la sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

Por consiguiente, esta Agencia que el procedimiento de acceso a los datos personales obrantes en el Registro que mejor se adecúa a la normativa sobre protección de datos personales es el contemplado en la letra b, el acceso en línea, para el cual el precepto establece unas garantías adicionales, sin perjuicio del resto de garantías que deban adoptarse conforme a lo que se señalará en el apartado siguiente. No obstante, también en este supuesto se deberán adoptar las medidas técnicas y organizativas que garanticen el cumplimiento del citado principio de minimización, de modo que se acceda a los datos estrictamente necesarios para verificar la existencia, vigencia y alcance del poder en relación con la concreta actuación administrativa que se pretende realizar y para poder comunicarse con el representante.

Todo ello sin perjuicio de que deban arbitrarse otras medidas que permitan, respetando igualmente el citado principio de minimización, acceder a los datos en los casos de fallo del sistema y siempre que, por razones de urgencia, no pueda esperarse al restablecimiento del mismo, debiendo preverse las garantías oportunas.

V

Otra diferencia significativa entre la presente Orden y las que regulan el Registro electrónico de apoderamientos y el Registro electrónico general de la AGE es que la misma **no contiene en su articulado referencia alguna a la protección de datos personales, ni incluye un artículo que se refiera específicamente a la protección de datos de carácter personal**. **Por ello, se considera necesario introducir dicho precepto, en el que deberán tenerse en cuenta, igualmente, lo manifestado por esta Agencia al informar dichas órdenes en los citados informes 4/2021 y 5/2021.**

Para ello, deberá identificarse la base jurídica del tratamiento, teniendo en cuenta que, en relación con el tratamiento de datos por parte de las Administraciones Públicas, es criterio reiterado de esta Agencia que el fundamento del mismo debe encontrarse en las letras c) y e) del artículo 6.1 del RGPD. En este sentido, en el informe 175/2018 ya se señalaba lo siguiente:

> Como CONCLUSIÓN en este punto, cabe decir que, con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según los casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD).

No obstante, en el Informe 74/2019, se destacaba la necesidad de deslindar ambos conceptos, ya que no hacerlo así implicaría confundir, en la práctica totalidad de los casos de actuación de la Administración, ambas bases jurídicas, concluyendo que

> Por ello, la base jurídica prevista en la letra c) del artículo 6.1. del RGPD será de aplicación en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal, y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público (artículo 103 de la Constitución).
>
> Y el criterio que viene manteniendo reiteradamente esta Agencia, en relación con los registros administrativos, es que el tratamiento de los datos personales correspondientes se encontraría se encontraría amparado por lo dispuesto en la letra e) del artículo 6.1.del RGPD: “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”, siempre que se haya establecido por una norma con rango de ley, conforme a lo señalado por el artículo 8.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: “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” (Informe 92/2020, en relación con el Registro de Variedades Protegidas y el Registro de Variedades Comerciales o el Informe 128/2018 sobre el registro unificado sobre certificados y centros de formación de gases fluorados).

En el presente caso, siendo el procedimiento administrativo el “conjunto ordenado de trámites y actuaciones formalmente realizadas, según el cauce

legalmente previsto, para dictar un acto administrativo o expresar la voluntad de la Administración", configurándose, de acuerdo con la doctrina del Tribunal Supremo, como una garantía para los particulares (sentencia del Tribunal Supremo de 20 de septiembre de 1983), y estando la Administración obligada a asistir en el uso de medios electrónicos a los interesados que no estén obligados a relacionarse de ese modo con la misma y que así lo soliciten, especialmente en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas (artículo 12.2 de la Ley 39/2015), la habilitación exigida legalmente a los funcionarios que realicen dichas funciones, de acuerdo con los artículos 12 y 27 de la misma y su inscripción en el Registro y, consecuentemente, el tratamiento de sus datos personales necesarios para dicha inscripción resultaría necesario para el adecuado funcionamiento de la Administración electrónica y las administraciones públicas puedan ejercer las potestades que tienen atribuidas. De este modo, además del cumplimiento de la obligación legal impuesta por el artículo 12 y por el artículo 27 de la Ley 39/2015, el tratamiento también se encontraría legitimado, de este modo, en el artículo 6.1.e) del RGPD: "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". Asimismo, dicho tratamiento derivaría, igualmente, de la relación estatutaria a la que están sujetos los funcionarios públicos, por lo que también se encontraría legitimado por la letra b) del citado precepto: "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales".

Por consiguiente, en el presente caso concurrirían tres bases jurídicas que legitiman el tratamiento, al amparo de las letras b), c) y e) del RGPD.

Todo ello, sin perjuicio del deber de informar a los afectados en los términos previstos en el artículo 13 del RGPD, pudiendo realizarse dicha información "por capas", conforme al artículo 11 de la LOPDGDD.

Por otro lado, debe hacerse especial referencia a las medidas de seguridad que deben adoptarse para salvaguardar el derecho a la protección de datos, al no existir ya, a diferencia de lo que ocurría en el momento de aprobación de la Ley 39/2015, un elenco cerrado de las mismas establecido por la legislación de protección de datos.

En este punto, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos

Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Así, el artículo 24.1 del Reglamento General de Protección de Datos dispone que “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual “Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el

tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

A su vez, en relación con la seguridad de los datos personales, el artículo 32.1 establece que "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

Un papel fundamental, en fin, dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el Delegado de Protección de Datos, que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un Delegado en los supuestos en que "el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial".

A su vez, el artículo 38.1 establece claramente que "El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales" y el artículo 39.2 dispone que "El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento".

Finalmente, el artículo 39.1 enumera las funciones del delegado de Protección de Datos, entre las que se encuentran ""informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros" (apartado a), "supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes" (apartado b) y "ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).

De lo que acaba de indicarse se desprenden dos conclusiones: por una parte, la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone la necesidad de realizar un análisis de riesgos en materia de protección de datos y, en su caso una evaluación de impacto en

la misma, sin que sea suficiente una mera remisión a las normas de protección de datos, habida cuenta que éstas ya no establecen un modelo tasado de cumplimiento.

Por otra, el Delegado de Protección de Datos, obligatorio en el supuesto que ahora se está analizando, deberá asesorar en dicho análisis y en la adopción de las medidas necesarias, en virtud de las funciones que el Reglamento General de Protección de Datos le otorga expresamente.

Por ello debería hacerse constar expresamente en el precepto que, previo análisis de los riesgos para los derechos y libertades de las personas físicas, 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 que serán revisadas y actualizadas cuando sea necesario.

Además, debería clarificarse en dicho precepto que las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

Por otro lado, otro de los principios recogidos en el artículo 5 del RGPD en su letra d) es el de exactitud de los datos, lo que impone al responsable la obligación de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. A estos efectos, la única previsión que se contiene es la prevista en el apartado 3 del artículo 7, de modo que “se podrá consultar la base de datos del Registro Central de Personal o sistema equivalente, únicamente a efectos de la comprobación de los datos de la situación administrativa y del destino de los funcionarios habilitados”, señalando en su apartado 4 que “La inscripción de la habilitación continuará vigente hasta que se cancele la misma en el Registro de funcionarios habilitados, en los supuestos contemplados en el apartado segundo, o hasta que transcurra el periodo máximo de vigencia sin solicitud expresa de prórroga”.

Por ello, debería recogerse, bien en el artículo 5 o en el precepto dedicado a la protección de datos personales, la necesidad de adoptar las medidas que se estimen adecuadas para garantizar que la cancelación de las inscripciones y, en su caso, la rectificación de los datos personales, se realizarán sin dilación teniendo en cuenta que se trata de datos personales correspondientes a funcionarios públicos que se encuentran en poder de la Administración. Una de dichas medidas debería ser, tal y

como se recoge en el artículo 4.5. de la Orden HAP/7/2014, de 8 de enero que "si se detectan cambios en alguna de las circunstancias bajo las cuales se realizó la habilitación, desde el Registro Central de Personal se informará al Registro de funcionarios habilitados para que suspenda la habilitación y lo ponga en conocimiento del órgano que realizó la inscripción del funcionario".

VI

Por otro lado, debe hacerse especial referencia a la previsión contenida en el artículo 3.2 de la Orden, que desarrolla las previsiones sobre identificación y firma electrónica, partiendo de la necesidad de contar con el consentimiento expreso del interesado.

A este respecto, el artículo 12, en su apartado 2 *in fine* de la Ley 39/2015 prevé que "será necesario que el interesado que carezca de los medios electrónicos necesarios se identifique ante el funcionario y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia para los casos de discrepancia o litigio"

Dicho precepto no establece dónde deberá custodiarse dicha constancia, aunque lo lógico es pensar que, dada su finalidad de acreditar dicha circunstancia en el supuesto de discrepancia o litigio, la misma deberá custodiarse por el órgano administrativo competente para la tramitación del correspondiente procedimiento administrativo, como uno de los documentos incorporados al expediente, tal y como prevé el artículo 16.5 al referirse a los documentos presentados de manera presencial, que deberán ser digitalizados "para su incorporación al expediente administrativo electrónico ". Asimismo, el artículo 39.6 del proyecto de Real Decreto de desarrollo prevé que "el archivo de los documentos intercambiados por registro corresponderá al órgano competente para la tramitación del procedimiento, de acuerdo al plazo que determine su normativa".

Sin embargo, el texto del artículo 3.2. de la Orden dispone lo siguiente:

> El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado así como una copia del documento de consentimiento expreso cumplimentado y firmado, del que quedará constancia en el Registro regulado en esta Orden. La información contenida en el Registro de funcionarios habilitados y la copia de la documentación relacionada con las actuaciones de los funcionarios habilitados se conservarán, en los términos que establezca la legislación aplicable, en el expediente electrónico del procedimiento administrativo, a los efectos de prueba en los procedimientos administrativos o judiciales que puedan tener lugar.

Por consiguiente, el precepto prevé, por un lado, que se deje constancia del documento de consentimiento expreso en el Registro de funcionarios habilitados, al tiempo que se prevé que el mismo formará parte, junto con el resto de documentación, en el expediente electrónico del procedimiento administrativo a los efectos de prueba en los procedimientos administrativos o judiciales que puedan tener lugar. Y en las cláusulas informativas del documento de consentimiento expreso que se recogen en el Anexo I, después de indicar que la finalidad del tratamiento es la de "acreditar el consentimiento expreso del ciudadano a la habilitación del funcionario en los términos fijados por el Art. 12 de la Ley 39/2015, de 1 de octubre" señala que "los datos personales recogidos a través de este formulario serán custodiados por la unidad en la que el ciudadano haya comparecido para realizar el trámite o actuación administrativa".

Por consiguiente, los datos personales del interesado contenidos en el documento de consentimiento expreso quedarían reflejados en el Registro de habilitados, en el expediente administrativo y en la propia unidad en la que haya comparecido.

Como hemos visto, el Registro de habilitados tiene por finalidad acreditar dicha habilitación, a cuyo objeto deberán inscribirse los funcionarios que señala el artículo 2, inscripción que se realizará por el órgano designado conforme al artículo 6.2. **Por consiguiente, al recogerse la constancia en el Registro de los consentimientos expresos, se estarían incorporando al Registro los datos personales de los interesados, lo que no se corresponde con la finalidad del Registro y sería contrario a los principios de limitación de la finalidad y minimización de datos, por lo que, a juicio de esta Agencia, debería suprimirse dicha incorporación, salvo que se considere imprescindible la misma, lo que requeriría su justificación de forma motivada en la MAIN y la modificación del texto de la Orden para adecuar la finalidad del Registro, de las inscripciones que deben realizarse y los órganos competentes para su realización.**

En este mismo sentido ya se había pronunciado esta Agencia en su Informe 425/2011:

> Ello plantea el problema de la discordancia existente entre el articulado del Proyecto y el contenido del mencionado Anexo y del propio Anexo III, puesto que si bien el contenido del articulado prevé que el Registro incorporará los datos de los funcionarios, siendo su finalidad la delimitación de los que se encuentran habilitados para la identificación y autenticación de los ciudadanos, finalidad que se reproduce a su vez en el citado Anexo III, del contenido establecido en este Anexo se deriva

que la finalidad del Registro excederá de la declarada, incorporando la información referida a los ciudadanos efectivamente identificados y autenticados, cuyos datos serán efectivamente incluidos en el fichero.

De este modo, y sin que ello suponga considerar que el tratamiento de los datos de los ciudadanos en el registro no resulte amparado por la Ley Orgánica 15/1999, sería necesario modificar el Proyecto en el sentido de o bien excluir la información de los ciudadanos de dicho Registro, lo que implica modificar la referencia a esa inclusión contenida en el Anexo I y las efectuadas por su parte por el Anexo III, o bien modificar el articulado del Proyecto en el sentido de especificar que el registro incorporará información de los ciudadanos identificados y autenticados y que su finalidad será igualmente la de acreditar la efectiva identificación y autenticación llevada a cabo, estableciendo asimismo el procedimiento de inclusión de las identificaciones y autenticaciones realizadas y los posibles accesos que pudieran realizares respecto de esos datos; en los mismos términos deberían modificarse los correspondientes apartados del Anexo III del Proyecto.

De este modo, sólo será posible la emisión de un informe favorable al Proyecto en caso de que se proceda a su modificación para lograr la correlación entre la finalidad y contenido del Registro en los términos establecidos en su articulad y la que se deriva de su Anexo, a fin de que pueda valorarse la existencia de una adecuada legitimación para el tratamiento de los datos de los ciudadanos objeto de identificación y autenticación.

Por último, **deberán revisarse los Anexos para adecuarlos a las observaciones realizadas en el presente informe, debiendo desarrollarse las cláusulas informativas de modo que incluyan toda la información prevista en el artículo 13 del RGPD, pudiéndose ofrecer “por capas”, conforme al artículo 11 de la LOPDGDD.**