- **Expediente N.º: EXP202102432**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 4 de agosto de 2021, ***A.A.A.*** (en adelante, la parte reclamante) 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES. SUBDIRECCIÓN GENERAL DE RECURSOS HUMANOS E INSPECCIÓN GENERAL DE SERVICIOS, con NIF S2801449F (en adelante, el Ministerio). Los motivos en que basa la reclamación son los siguientes:

El reclamante manifiesta que la Subdirección General de Recursos Humanos e Inspección de Servicios ha remitido por correo electrónico a un tercero el Oficio de contestación de la Subdirección General de Recursos Humanos e Inspección de Servicios, del Ministerio de Inclusión, Seguridad Social y Migraciones, en el que se resolvía su solicitud de cese y en la que se reflejaban aspectos e información relacionada con sus circunstancias laborales y que ha permitido su identificación, vulnerando la confidencialidad en el tratamiento de sus datos.

Junto a la reclamación se aporta:

- Escrito de 15 de junio de 2021, en el que solicita se dicte resolución por la que se le cese en su puesto y, en su caso, se emita informe sobre todas las Libres Designaciones que se hayan producido dentro del ******PUESTO.1*** en los últimos 4 años.

- Oficio de contestación por la Subdirección General de Recursos Humanos e Inspección de Servicios, del Ministerio de Inclusión, Seguridad Social y Migraciones, de 23 de julio de 2021.

- Imagen del correo electrónico enviado por la citada Subdirección General al reclamante remitiendo el Oficio de contestación, de 26 de julio de 2021.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación al Ministerio, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada

conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 11 de octubre de 2021, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 27 de octubre de 2021. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 16 de diciembre de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Hechos según manifestaciones de la parte reclamante:

(...)

Fecha en la que tuvieron lugar los hechos reclamados: 22 de julio de 2021.

En respuesta al requerimiento de información, el representante del Ministerio pone de manifiesto lo siguiente:

(...)

QUINTO: Con fecha 28 de octubre de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al Ministerio, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificadas en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD respectivamente.

SEXTO: Con fecha 11 de noviembre de 2022, el Ministerio presenta un escrito a través del cual solicita copia del expediente, así como la ampliación del plazo para aducir alegaciones.

SÉPTIMO: Con fecha 14 de noviembre de 2022, el órgano instructor acuerda la ampliación de plazo instada hasta un máximo de cinco días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP.

El acuerdo de ampliación se notifica al Ministerio ese mismo día, como consta en el acuse de recibo que obra en el expediente.

OCTAVO: Con fecha 22 de noviembre de 2022, se recibe en esta Agencia, en tiempo y forma, escrito del Ministerio en el que aduce alegaciones al acuerdo de inicio en el que, en síntesis, manifiesta que:

Primero. - Error administrativo y conducta proactiva de inmediata rectificación.

El Ministerio admite que, por un error humano, una resolución que resolvía una solicitud de información del reclamante fue dirigida en el encabezamiento del escrito, y consecuentemente notificada, a otra persona, figurando el nombre y apellidos de éste.

Entiende que el error sería calificable jurídicamente como mero error material, consistente en cambiar un nombre y apellidos por otro nombre y apellidos en una resolución, y que el mismo fue inmediatamente detectado y se procedió a su inminente subsanación mediante rectificación de la resolución y remisión del oficio a su correcto destinatario, todo ello en el transcurso de dos días hábiles. Se adjunta el documento subsanado, firmado el día 23/07/2022

Segundo. - Similitudes concurrentes que facilitaron la comisión de error material.

Indica el Ministerio que la confusión de un nombre (el del reclamado) por otro (C.C.C.) en el encabezamiento como destinatario del oficio administrativo tiene como origen la circunstancia de que se estaban resolviendo dos solicitudes que compartían numerosas similitudes:

(…)

El jueves 22/07/2021 se envió el oficio dirigido al C.C.C. cuyo contenido se correspondía con la solicitud de cese y de información pública presentada por el reclamante.

Dos días (hábiles) después, el lunes 26/07/2021, se subsanó el error mediante la notificación del oficio a su correcto destinatario.

Tercero. - Información solicitada por el reclamante.

Señala el Ministerio que, tal y como consta acreditado (páginas 7 a 15 del expediente administrativo), la solicitud del reclamante consiste en 3 peticiones, en extracto, las siguientes:

> 1. “Que se dicte resolución de cese.
> 2. Que, subsidiariamente, se dicte resolución expresa que fundamente no dar efectividad (…)
> 3. Que “Para el caso anterior, se interesa, previo a su solicitud al Consejo de Transparencia, se emita informe sobre todas las Libres Designaciones que se hayan producido dentro del ***PUESTO.1 en los últimos cuatro años, con

referencia a los informes favorables o desfavorables que se hayan emitido en cada una de ellas".

Cuarto. - Desacuerdo con la valoración de los hechos por parte del reclamante.

El Ministerio, entrando a una valoración más pormenorizada de los hechos relatados por el reclamante en el apartado "Descripción de los hechos" en el Anexo 1 (página 8 del expediente administrativo), entiende que no son fiel reflejo de la realidad, por los siguientes motivos:

1. Contrariamente a lo que expone el reclamado *<<En dicho oficio, que ha trascendido a otra provincia, a otro servicio jurídico y a otros compañeros (…)>>.* Dicho oficio únicamente fue notificado a una persona, no a varios compañeros y, a priori, resulta indiferente el hecho de que esté ubicado en otra provincia o servicio jurídico. La información revelada no causa verdadero perjuicio al interesado, por lo que no debería considerarse con entidad de brecha de seguridad/confidencialidad.

2. La firma de una carta colectiva dirigida a un cargo público, concretamente a la Directora del Servicio Jurídico, no constituiría en sí una información de carácter personal, pues no es un documento de carácter privado ni personal del reclamante. No se aprecia tampoco riesgo alguno de dejarle expuesto en una situación incómoda o delicada por el hecho de afirmar que no existen suficientes efectivos, circunstancia que es continuamente denunciada por empleados y sindicatos respecto de diversos servicios y administraciones públicas (servicios sanitarios, Seguridad Social, etc.)

3. La información sobre libres designaciones en los últimos 4 años se facilita en ejercicio del derecho de acceso a la información, previsto en el artículo 105.b) de la Constitución y constituye información pública de conformidad con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno.

Tal y como se define en el artículo 13 de la Ley 19/2013, de 9 de diciembre, se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título (Título I) y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Los procesos de provisión de puestos de trabajo en las administraciones públicas están sometidos, entre otros, a los principios constitucionales de publicidad, igualdad, concurrencia, etc, desarrollados en el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto Básico del Empleado Público y normativa concordante.

La información facilitada no incluye datos de carácter personal, es pública y no pone de manifiesto una supuesta existencia de buena o mala relación personal con la Dirección del Servicio Jurídico.

4. En el oficio objeto de reclamación no se aprecia referencia alguna a supuestas <<*diatribas administrativas y judiciales que actualmente mantengo con ellos*>>. Se trata de una afirmación de alcance incierto y sin aparente fundamento.

5. Incierta también es la supuesta vinculación entre el error humano y el medio de notificación, pues de haberse notificado el oficio por medio distinto al correo electrónico, por ejemplo, a la Carpeta Ciudadana de quien aparece en el oficio como destinatario, igualmente hubiese accedido ***B.B.B.***, mediante su certificado electrónico, a la resolución.

El error está en la consignación del nombre, no en la vía por la que se practicó la notificación.

A la vista de lo anterior, concluye el Ministerio que la versión que de los hechos que ofrece el reclamante es subjetiva, distorsionada, y pudiese corresponderse con una actitud reactiva por no haber obtenido su pretensión administrativa, esto es, el cese en su puesto para ocupar otro puesto en otra administración.

Quinto.- Valoración de la información del reclamante, facilitada a un tercero.

Señala el Ministerio que, a la vista del contenido de la resolución dirigida por error al C.C.C. (pág. 16 a 19 del expediente administrativo) se aprecia que:

1. No consta ningún dato personal del reclamante.

2. La información sobre la adjudicación del puesto del Ayuntamiento de Madrid, es pública y notoria, y así consta publicada en el ******BOLETIN.1***. Efectivamente es un elemento identificable, pero es información pública.

3. La información referida a las circunstancias del reclamante puesta a disposición del C.C.C., no desvela ninguna información de la que no tuviese ya conocimiento, por el contrario viene a confirmar la unidad de criterio en la resolución de un supuesto de hecho coincidente con el del destinatario, pues en idénticas circunstancias que él, el MISSM ha resuelto en el mismo sentido y con la misma motivación: no se resuelve favorablemente la solicitud de cese por haber sido informado en sentido desfavorable por parte del Servicio Jurídico del INSS.

4. El resto de información, relativa a los informes emitidos referentes a los nombramientos en libre designación producidos en los cuatro últimos años dentro del ***PUESTO.1 es información pública que no contiene ningún dato de carácter personal.

Sexto. Calificación jurídica.

Indica el Ministerio que en el acuerdo de inicio del procedimiento sancionador se califican los hechos como presunta infracción del artículo 5.1.f, tipificada en el artículo 83.5 y, también, la presunta infracción del artículo 32, tipificada en el artículo 83.4 del Reglamento General de Protección de Datos (RGPD).

La comisión de ambas infracciones tiene prevista la imposición de sanción de apercibimiento.

El Ministerio considera, sin embargo, que a los hechos no les resultaría de aplicación dicha calificación por los siguientes motivos:

> 1. No incurre en la infracción prevista en el artículo 5.1.f) del RGPD porque el error humano consistente en dirigir un oficio a nombre de otra persona, por parte de la funcionaria que tramitaba y resolvía dos expedientes administrativos que guardaban entre sí identidad sustancial e íntima conexión no podría haberse evitado mediante la adopción de distintas medidas de seguridad, ya fuesen de carácter técnico o de cualquier otra naturaleza, en el tratamiento y en materia de protección de datos de carácter personal.
>
> 2. Tampoco se encuadrarían los hechos en la infracción de las previsiones establecidas en el artículo 32 del RGPD porque, en el mismo sentido, la aplicación de medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo no podía haber impedido la confusión de una funcionaria en la asignación del nombre del destinatario de un oficio.
>
> Efectivamente, teniendo en cuenta el estado de la técnica, costes de aplicación, naturaleza, alcance, contexto, fines del tratamiento, etc.., las medidas técnicas y organizativas que se pudiesen aplicar, tales como seudonimización, cifrado de datos personales, procesos de verificación y evaluación regular de la eficacia para garantizar la seguridad del tratamiento, u otras medidas técnicas, organizativas o de naturaleza análoga, no hubiesen podido impedir el error humano cometido a partir de las numerosas similitudes y puntos de coincidencia entre dos expedientes administrativos que se estaban resolviendo simultáneamente.

Por ello, señala el Ministerio que la calificación jurídica que merece el presente supuesto de hecho se encuentra previsto en el artículo 109.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece, en relación con la revocación de actos y rectificación de errores, que:

> *2. Las Administraciones Públicas podrán, asimismo, rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos existentes en sus actos.*
>
> La ley procedimental regula este tipo de errores materiales con carácter general, dada su comprensible e inevitable concurrencia en la tramitación ordinaria de los procedimientos administrativos.

En base a todo lo anterior, el Ministerio concluye que:

> 1. El incidente tiene su origen en la confusión en el nombre del destinatario de un oficio, en el contexto de resolución de dos expedientes que guardan identidad sustancial e íntima conexión.

No se aprecia grave perjuicio al interesado que justifique la calificación de este incidente como “brecha de seguridad o de confidencialidad”.

2. El contenido de la información revelada es de carácter eminentemente público, sin que se hayan visto comprometidos datos de carácter personal, ni puedan calificarse de sensibles o relevantes.

3. Se actuó proactivamente y sin dilación, mediante la inmediata rectificación de oficio del error cometido.

4. Al margen de todas las medidas de seguridad previstas, el error humano es inevitable al 100%, aun tratándose, en este caso, de una funcionaria de reconocida competencia y diligencia profesional.

5. No obstante, se tratará de identificar medidas procedimentales para evitar que en un futuro vuelvan a ocurrir situaciones similares.

En virtud de lo expuesto, solicita el Ministerio que se acuerde el archivo del expediente incoado por presuntas infracciones previstas en los artículos 5.1.f y 32 del RGPD

NOVENO: con fecha 6 de junio de 2023, el órgano instructor del procedimiento sancionador formuló propuesta de resolución, en la que propone que por la Directora de la AEPD se imponga a MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES, con NIF S2801449F:

-por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de APERCIBIMIENTO

-por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO

Esta propuesta de resolución, que se notificó al Ministerio conforme a las normas establecidas en la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 7 de junio de 2023, como consta en el acuse de recibo que obra en el expediente.

En dicha propuesta de resolución, frente a las alegaciones formuladas por el Ministerio, se dio la siguiente respuesta:

Primero. - Desacuerdo con la valoración de los hechos

En este apartado se procede a aglutinar alegaciones del Ministerio relativas a que, por un lado, no está de acuerdo con la valoración de los hechos realizada por el reclamante, y por otro, que no se han visto afectados datos personales y que, además, es información pública.

Frente a ello, procede señalar que, a pesar de que el reclamante pueda referirse a una pluralidad de destinatarios o a cualesquiera otras consideraciones subjetivas, el presente procedimiento sancionador se tramita por haber comunicado datos

personales a un tercero no autorizado, es decir, a una única persona y vulnerando, con ello, el deber de confidencialidad de los datos personales.

En cuanto a que la información revelada no causa grave perjuicio al reclamante, procede señalar que el perjuicio se encuentra ínsito en la propia vulneración de la confidencialidad de los datos, pues ello implica una pérdida de control y de poder de disposición de los mismos, suponiendo ello una vulneración del derecho fundamental a la protección de los datos personales.

Debe recordarse que, de conformidad con la normativa en materia de protección de datos, los datos personales están sujetos a un deber de confidencialidad y los mismos no pueden ser comunicados a un tercero salvo que medie consentimiento del titular de los datos o concurra alguna otra de las circunstancias que hacen lícito el tratamiento, de conformidad con el artículo 6.1 del RGPD.

En cuanto a lo manifestado por el Ministerio, relativo a que la información revelada no contiene datos de carácter personal, se indica, por el contrario, que la información sobre determinadas circunstancias de índole laboral, como solicitudes de cese realizadas por el reclamante, la denegación de los mismos, así como las solicitudes y denegación de las preceptivas autorizaciones en relación con la provisión de puestos de trabajo en la Administración Pública, son datos personales, pues son información relativa a una persona identificada y que, además, no son datos públicos, como entiende el Ministerio y ello con independencia de que la adjudicación final de los puestos de trabajo deban ser publicados en el Boletín Oficial correspondiente (pero no así las autorizaciones, ceses, denegaciones, errores de tramitación y demás trámites y vicisitudes que forman o pueden formar parte del proceso).

Segundo. - Calificación jurídica

Sostiene el Ministerio en este apartado que los hechos no suponen infracción del artículo 5.1.f) ni del artículo 32 del RGPD, por cuanto se debió a un error humano, calificado como un mero error material regulado en el artículo 109.2 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

Frente a ello, debe señalarse que no nos encontramos ante un error material contenido en un acto administrativo (el cual es susceptible de subsanación mediante otro acto administrativo), sino ante una vulneración de la confidencialidad de datos personales que fueron comunicados a un tercero no autorizado. Por tanto, el error aducido por el Ministerio no estaría en el contenido del Oficio (acto administrativo) enviado, sino en haberlo enviado a otra persona y no a su destinatario, vulnerándose con ello, como se ha indicado, la confidencialidad de los datos personales contenidos en dicho Oficio.

Por todo lo expuesto, se desestiman las alegaciones formuladas.

DÉCIMO: Con fecha 21 de junio de 2023, se recibe en esta Agencia, en tiempo y forma, escrito del Ministerio en el que aduce alegaciones a la propuesta de resolución en el que, en síntesis, manifiesta que:

Primera. Ausencia de culpabilidad
Alega que no puede considerarse que ha actuado de manera dolosa, imprudente, negligente o de ignorancia inexcusable, en correlación con la normativa sobre protección de datos.

Así, sostiene que la circunstancia desencadenante del quebranto de la confidencialidad del dato devino de un simple error material, inducido en parte, por las circunstancias concurrentes del caso, que se ocasionó por la tramitación simultanea de dos solicitudes que compartían multitud de similitudes.

Entiende que no se ha razonado la existencia de culpabilidad hacia el Ministerio. Esta falta de culpabilidad, junto con el error de considerar que habiéndose adoptado medidas de seguridad se hubiese evitado el quebranto de la confidencialidad, cuando estamos frente a un error humano inducido por las circunstancias concurrentes del caso, donde no existen medidas de seguridad razonables acorde al riesgo que hubiesen supuesto o hubiesen permitido una mitigación de la amenaza, supone una aplicación arbitraria de la legalidad y la exigencia de una responsabilidad objetiva.

Esta cuestión resulta de especial relevancia y constituye uno de los Principios por los que ha de regirse la potestad sancionadora, y así, el artículo 28 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, establece que "1. *Sólo podrán ser sancionados por hechos constitutivos de infracciones administrativas las personas físicas y jurídicas […] que resulten responsables de los mismos a título de dolo o culpa*".

Invoca la Sentencia del Tribunal Constitucional n.º 246/1991, de 19 de diciembre, que indica: *«(...) En concreto, sobre la culpa, este Tribunal ha declarado que, en efecto, la Constitución española consagra sin duda el principio de culpabilidad como principio estructural básico del Derecho Penal y ha añadido que, sin embargo, la consagración constitucional de este principio no implica en modo alguno que la Constitución haya convertido en norma un determinado modo de entenderlo (STC 150/1991). Este principio de culpabilidad rige también en materia de infracciones administrativas, pues en la medida en que la sanción de dicha infracción es una de las manifestaciones del ius puniendi del Estado resulta inadmisible en nuestro ordenamiento un régimen de responsabilidad objetiva o sin culpa (STC 76/1990)*».

Indica el Ministerio que el concepto de riesgo 0 no existe. Que siempre existe un riesgo inherente que, una vez se han aplicado las medidas y garantías, se minimiza, permaneciendo un riesgo residual. Así todas las actividades de tratamiento de datos personales implican siempre un riesgo para las personas cuyos datos son tratados y, en particular, para sus derechos y libertades. Incluso, en aquellos casos en los que el responsable, ya sea por la tipología del dato o por el tipo de actividad de la organización, pudiera asumir la existencia de un riesgo escaso para los interesados, sin que ello suponga la aplicación automática del régimen sancionador si se materializa dicho riesgo residual.

En el presente caso, estamos en un escenario de riesgo residual y más concretamente en lo relativo o referente a los derechos y libertades de la persona afectada. La difusión del dato no se materializó sobre una multitud de personas descontroladas. Tampoco se publicó la información a través de canales abiertos. Los daños y

perjuicios sobre el afectado son muy relativos. No hay riesgo de discriminación, usurpación de identidad, fraude, pérdidas financieras o daños reputacionales. Fue simple y llanamente el envío de un correo electrónico sobre una única persona, identificada y sometida a cláusulas de confidencialidad y deber de secreto profesional. Un simple caso fortuito.

A su vez se actuó con extrema celeridad para mitigar el impacto, procediendo a su inminente subsanación mediante rectificación de la resolución, puesta a la firma del entonces Subdirector General y remisión del oficio a su correcto destinatario.

Sostiene el Ministerio que en todo lo relativo al tratamiento de sus datos personales, está plenamente comprometido con la legislación vigente en materia de protección de datos personales. En su función de responsable del tratamiento de datos de carácter personal, trata los datos personales de su titularidad para las finalidades específicas y con la confidencialidad debida, observando las obligaciones que la regulación de la protección de datos de carácter personal impone, con atención especial a las medidas de índole técnico y organizativo para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos tratados y los riesgos a los que están expuestos.

En cumplimiento del citado compromiso del Ministerio con la protección de los datos, indica que cuenta con:

- Política y procedimientos internos para regular el tratamiento de los datos de carácter
personal.
- Un Inventario / Registro de Actividades de Tratamiento publicada en nuestra sede electrónica (https://sedemissm.seg-social.es/proteccion-de-datos)
- Una Delegada de Protección de Datos, como piedra angular del modelo de gobierno de la protección del dato.
- Una oferta adecuada de formación y concienciación en protección de datos a empleados y personal del Ministerio.
- Unos canales internos debidamente habilitados para que puedan realizarse consultas, quejas y ejercicio de derechos.
- Realización de análisis de riesgos y de Impacto de la Privacidad.

Y que desde la perspectiva de la confidencialidad recogida en el artículo 5 de la LOPDGDD, cuenta con una serie de medidas vinculadas y/o asociadas con la dimensión de la confidencialidad, entre otras:

- Sistemas de identificación y autenticación.
- Se han definido los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo en términos de confidencialidad.
- Se ha implantado un deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación a través de las correspondientes cláusulas.
- Se aplica la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas.

- Se han aplicado sobre los sistemas de tratamiento medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, con capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente.

Por tanto, sostiene que solo pueden ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos. En el caso concreto, nos hallamos ante la comisión de un error humano por parte de una funcionaria que no ha tratado en ningún momento de evadir el cumplimiento de los protocolos y procedimientos.

Indica también que la instrucción no delimita en su propuesta de resolución si el resultado se produjo por dolo o por culpa. Tampoco determina el tipo de medida y/o requisitos de seguridad que, de haberse implantado, el resultado hubiese sido otro. Básicamente porque no existe medida racional que teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza del riesgo, permita mitigar el error humano, siendo éste un factor de los más difíciles de prever dada la complejidad de la naturaleza humana, así como otros factores vinculados a éste como son los procedimientos, el contexto operativo que afecta a los operadores humanos o los elementos de gestión que promueven la falibilidad humana. Simplemente se sanciona desde el resultado.

Así por ejemplo lo ha declarado el Tribunal Constitucional en Sentencia 164/2005 de 20 de junio al afirmar que "no se puede por el mero resultado y mediante razonamientos apodícticos sancionar, siendo imprescindible una motivación específica en torno a la culpabilidad o negligencia y las pruebas de las que ésta se infiere". También, en este sentido la Audiencia Nacional estima en Sentencia de 26 de abril de 2002 (Rec. 895/2009) que: “En efecto, no cabe afirmar la existencia de culpabilidad desde el resultado”.

Segunda: Propuesta de sanción contraria al Principio de Proporcionalidad.

Entiende el Ministerio que la propuesta de resolución sancionadora no atiende tampoco al principio de proporcionalidad planteando la imposición de dos sanciones de apercibimiento por un simple error humano.

En cuanto a la sanción propuesta, indica que no concurren los requisitos de graduación de la sanción, ni se ajusta a los criterios previstos en la normativa, concretamente los relacionados en el apartado tercero del artículo 29 de la Ley 40/2015, de 1 de octubre, que dispone lo siguiente:

3. En la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá observar la debida idoneidad y necesidad de la sanción a imponer y su adecuación a la gravedad del hecho constitutivo de la infracción. La graduación de la sanción considerará especialmente los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora
c) La naturaleza de los perjuicios causados.

> *d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.*

En el presente supuesto, en el expediente sancionador, señala el Ministerio que:

> a) No ha concurrido culpabilidad ni intencionalidad por parte de la funcionaria que cometió el error en el acto de notificación
> b) No ha existido continuidad ni persistencia en la conducta infractora.
> c) La naturaleza o alcance de los perjuicios causados resulta interpretable.
> d) No se ha producido reincidencia.

En definitiva, arguye que la sanción propuesta, máxime tratándose de dos apercibimientos, resulta inadecuada, innecesaria y contraria al principio de proporcionalidad y criterios de graduación de la sanción.

No se aprecia en la instrucción finalidad correctiva o preventiva alguna, tan sólo el ánimo sancionador y de aplicación de un castigo, a todas luces excesivo y desproporcionado.

Tercera: Atipicidad de la conducta imputada

Alega el Ministerio que la descripción de los hechos y la calificación jurídica practicada no se subsume en ninguno de los supuestos definidos como infracción, como tampoco se dan las circunstancias objetivas y personales determinantes de la licitud y de la imputabilidad y que la Agencia Española de Protección de Datos a estos efectos recrimina que los datos han sido tratados de manera que no se garantiza una seguridad adecuada, mediante la aplicación de medidas técnicas u organizativas apropiadas (Integridad y Confidencialidad)

En este sentido, indica que el artículo 25.1 de la Constitución recoge la regla "*nullum crimen nulla poena sine lege*", que presenta una garantía material derivada del mandato de tasatividad (o de "lex certa"), concretada en la exigencia de que las conductas ilícitas –y las correspondientes sanciones– se encuentren predeterminadas normativamente.

Invoca lo indicado por el Tribunal Constitucional (cfr., a modo de ejemplo, su sentencia n.º 242/2005, de 10 de octubre), respecto a que esta garantía material «*implica que la norma punitiva permita predecir con suficiente grado de certeza las conductas que constituyen infracción y el tipo y grado de sanción de lo que puede hacerse merecedor quien la cometa». Aún es más ilustrativo lo que el propio Tribunal Constitucional tuvo ocasión de recordar en su auto n.º 148/2008, de 9 de junio: el principio de tipicidad «no sólo impide la imposición de sanciones por comportamientos ajenos a los previstos en la norma sancionadora sino que también prohíbe la analogía in peius y la interpretación extensiva in malam partem, es decir, la exégesis y aplicación de las normas fuera de los supuestos y de los límites que ellas mismas determinen (entre otras, SSTC 81/ 1995, de 5 de junio, F. 5 y 229/2007, de 5 de noviembre, F. 4), razón por la cual sólo se puede conectar la sanción prevista con las conductas que, por reunir todos los elementos del tipo descrito, son objetivamente perseguibles*».

El artículo 27 de la Ley 40/2015 de 1 de octubre recoge el principio de tipicidad que consiste en la necesidad de predeterminación normativa de las conductas infractoras y de las sanciones correspondientes. El principio de tipicidad se desenvuelve en el plano teórico mediante la plasmación explicita de los hechos constitutivos de la infracción y de sus consecuencias represivas en la norma legal. Pero en el terreno de la práctica, la anterior exigencia conlleva consigo la imposibilidad de calificar una conducta como infracción de sancionarla si las acciones u omisiones cometida por un sujeto no guardan una perfecta similitud con las diseñadas en los tipos legales.

Señala que no puede subsumirse la actuación del Ministerio bajo el tipo del artículo 5.1.f del RGPD, como la falta de adopción de medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32 del RGPD, cuando el Ministerio contempla todo un conjunto de medidas como las descritas en la alegación primera.

Entiende que no existe conexión directa en términos de tipicidad y culpabilidad entre el incumplimiento de las medidas de seguridad y el quebranto del deber de confidencialidad. El Ministerio implantó un sistema de seguridad que se vio vulnerado por un mero error humano, que a su vez, como se describió en el escrito de alegaciones a la incoación del procedimiento, nunca antes se había producido por parte de la funcionaria.

Indica que cumple escrupulosamente con dichos preceptos. En este sentido dos son los elementos nucleares que lo acreditan y que permite no subsumir los hechos bajo la conducta de vulnerar el deber de confidencialidad:

- El incidente no viene derivado porque un miembro del Ministerio haya incumplido su obligación de confidencialidad y deber de secreto porque haya difundido, divulgado información con datos de carácter personal sin base legitimadora. Sino simplemente por un mero error humano.
- Tampoco porque los sistemas no cuenten con sistemas de seguridad que no permita garantizar la confidencialidad del dato, ni porque su personal no tenga un compromiso o un deber de confidencialidad.

Señala el Ministerio que en nuestro ordenamiento jurídico no se permite que, en un caso como el que nos ocupa, pueda considerarse que los hechos acaecidos son constitutivos de infracción, tomando como fundamento un tipo infractor en el que no encaja la actuación del Ministerio.

Por todo lo que antecede, no existe acción u omisión por nuestra parte que guarde similitud con la falta de adopción de medidas técnicas adecuadas al riesgo para garantizar un nivel de seguridad adecuado, y por tanto no se puede subsumir nuestra conducta como una infracción de los artículos 5.1F y 32 del RGPD.

Cuarta. - Se reiteran todas las alegaciones hechas en anteriores escritos en el procedimiento de referencia.

Por todo lo anteriormente expuesto, solicita el Ministerio que se acuerde el sobreseimiento del expediente sancionador con el consiguiente archivo de las actuaciones.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Ha quedado acreditado que el Ministerio remitió un correo electrónico a un tercero (C.C.C.), (...), un Oficio de contestación a éste en el que aparecía información personal relacionada con sus circunstancias laborales (solicitud de cese, denegación de cese, etc), concretamente:

- Que ha sido nombrado para un puesto de libre designación en otra Administración Pública sin haberse seguido el procedimiento legalmente establecido, concretamente por la falta de informe previo favorable de la Administración de origen
- Que con fecha 4 de mayo de 2021, se informó al reclamante de un Informe desfavorable del INSS
- Que el reclamante reiteró la solicitud de informe al Ministerio y que se emitió nuevamente informe desfavorable de fecha 31 de mayo de 2021.
- Se indica la existencia de escrito de la Subdirección General de Recursos Humanos e Inspección de Servicios del Ministerio, de 4 de junio de 2021, por el que se comunica que no se procede a formalizar el cese del reclamante.
- Se indica que el reclamante ha solicitado que se informe sobre si existe o se está tramitando resolución expresa de su cese en la Administración de origen o, en su caso, si se ha interesado el cese diferido de tres meses, a lo que se le responde que no se va a proceder a formalizar su cese de conformidad con el escrito de 4 de junio de 2021
- Se indica que, subsidiariamente a lo anterior, el reclamante ha solicitado información en relación a los informes emitidos referentes a los nombramientos en libre designación producidos en los cuatro últimos años dentro del ***PUESTO.1.

SEGUNDO: De los datos contenidos en la carta de respuesta se deduce fácilmente la identidad del reclamante, pues en el mismo se indican los datos del puesto adjudicado y del Boletín donde se ha publicado. De hecho, ello es lo que permitió al tercero (C.C.C.) que recibió el oficio por error ponerse en contacto con el reclamante e informarle del ello.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el Ministerio realiza, entre otros tratamientos, la recogida, registro, conservación, utilización, acceso, supresión de los siguientes datos personales de personas físicas, tales como: nombre y apellidos, número de identificación, datos de contacto, número de teléfono, dirección de correo electrónico, circunstancias laborales, etc.

El Ministerio realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante brecha de seguridad) como “todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse enviado por correo electrónico un Oficio a un tercero conteniendo información sobre circunstancias laborales del reclamante, lo que supone una comunicación no autorizada de datos personales.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Alegaciones aducidas

En relación con las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas:

Primera.- Falta de culpabilidad

Aduce el Ministerio que no ha actuado ni con dolo ni con culpa en relación con la normativa sobre protección de datos pues insiste en que el quebranto de la confidencialidad devino de un simple error material de una persona inducido por las circunstancias concurrentes del caso, ya que se ocasionó por la tramitación simultánea de dos solicitudes con multitud de similitudes. Concluye por ello que el simple error humano no puede dar lugar a la atribución de consecuencias sancionadoras, pues constituiría una responsabilidad objetiva.

Asimismo, arguye el Ministerio que no existe medida de seguridad racional que permita mitigar el error humano, por lo que no procede deducir que la brecha de seguridad deriva de la falta de adopción de medidas de seguridad adecuadas ya que el incidente deriva de un simple fallo humano sobre el que no caben medidas de protección razonables acordes al riesgo, coste y naturaleza de la amenaza, tal y como exige el artículo 32 del RGPD, por lo que reitera que no existe culpabilidad, sino un simple caso fortuito.

Debe recordarse que el RGPD en el citado artículo 32 no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que: “(83) *A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. 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, como la destrucción, pérdida o*

alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

El Tribunal Supremo, en su Sentencia de 15/02/2022 (STS 543/2022), si bien indica que la obligación de diseñar e implantar las medidas de seguridad para evitar eventuales brechas de seguridad es una obligación de medios y no de resultado, señala también que no es suficiente el diseño de los medios técnicos y organizativos necesarios, sino que también resulta necesaria su correcta implantación y utilización de forma apropiada, de manera que el responsable también responderá por la falta de la diligencia en su utilización y aplicación. Al margen de que por un hecho fortuito o un acontecimiento de imposible previsión se cree una brecha de seguridad que el sujeto no hubiera podido evitar siquiera aplicando las más estrictas medidas.

Ahora bien, en el caso concreto, el Tribunal llegaba a la conclusión de que las medidas adoptadas por la recurrente no fueron suficientes y entendía que el estado de la técnica en el momento de los hechos permitía establecer medidas más oportunas y adecuadas. Indicaba finalmente el Tribunal que el hecho de que la filtración se produjera en última instancia por la actuación negligente de una empleada no eximía a la empresa de su responsabilidad. Por todo ello, confirmaba la sanción impuesta por la AEPD.

En el caso que nos ocupa, frente a la alegación relativa a que se debió a un simple error humano derivado de la similitud de los expedientes tramitados y que no existe medida de seguridad alguna para mitigarlo, procede señalar que, precisamente, en las Administraciones Públicas es habitual la tramitación de expedientes similares (a modo de ejemplo, solicitudes de subvenciones, prestaciones, procedimientos de provisión de puestos de trabajo, etc.) y que es justamente en ellos donde hay que valorar especialmente el riesgo del error humano.

En el presente caso, la confidencialidad se ha roto no como consecuencia de una actividad extraordinaria o inhabitual del Ministerio sino, por el contrario, en el seno de lo que se considera actividad normal, ordinaria y habitual del mismo.

El error humano es un riesgo que el responsable del tratamiento debe valorar cuando planifica el tratamiento, pues la posibilidad de equivocarse es intrínseca a la condición humana. El factor humano, la evidente posibilidad de cometer errores, es uno de los riesgos más importantes a considerar siempre en relación con la determinación de las medidas de seguridad. El responsable del tratamiento debe contar con el error humano como un riesgo más que probable. Los errores humanos se combaten y se mitigan desde el enfoque de riesgos, el análisis, la planificación, implantación y control de las medidas técnicas y organizativas adecuadas y suficientes.

Siempre hay posibilidad de implementar alguna medida procedimental para reducir el riesgo, para reducirlo al mínimo posible. Sin embargo, en el presente caso no se ha acreditado por parte del Ministerio una evaluación del riesgo que supone el error humano ni medida alguna implantada para mitigarlo, más allá de indicar, de forma genérica, que tiene implementadas medidas adecuadas en cumplimiento del artículo 32 y de afirmar que no existe medida alguna que mitigue o reduzca el error humano.

Por tanto, en el presente caso, la responsabilidad del Ministerio viene determinada por el incidente de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

En relación con la falta de culpabilidad alegada, se significa que el nacimiento de la responsabilidad sancionadora presupone la existencia de culpabilidad en cualquiera de sus manifestaciones: dolo, culpa o culpa levísima. En el ámbito del Derecho Administrativo Sancionador no es posible imponer sanciones basadas en la responsabilidad objetiva del presunto infractor porque las sanciones administrativas participan de la misma naturaleza que las penales, al ser una de las manifestaciones de la potestad punitiva del Estado y, como exigencia derivada de los principios de seguridad jurídica y legalidad penal consagrados en los artículos 9.3 y 25.1 de la CE, es imprescindible que este elemento esté presente como presupuesto para su imposición (STC 76/1999)

El principio de culpabilidad es exigido en el procedimiento sancionador, pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada. El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende "*que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable." El mismo Tribunal razona que "no*
basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia." (STS 23 de enero de 1998).
A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que "basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..." (SAN 29 de junio de 2001).

La Sentencia precitada conecta la reprochabilidad a una persona jurídica, de una determinada conducta, con el hecho de que aquella hubiera o no dispensado una eficaz protección al bien jurídico protegido por la norma. Atendidas las circunstancias del caso, es evidente que esa diligencia no se ha observado en relación con la remisión de una documentación a un tercero conteniendo datos personales a los que pudo acceder sin autorización de su titular.

Por tanto, la conducta del Ministerio ha de ser objeto de reproche consecuencia del incumplimiento de la normativa en materia de protección de datos personales, tanto por la vulneración del principio de confidencialidad, como por el quebrantamiento o ausencia de medidas técnicas y organizativas adecuadas, al permitir el acceso a los datos del reclamante sin autorización.

Lo anterior con independencia de que a posteriori el Ministerio haya tenido o no una actuación rápida en aras de mitigar el impacto de la vulneración de la confidencialidad. A este respecto, en cuanto a lo indicado por el mismo relativo a que procedió a su

inminente reparación mediante la rectificación de la resolución y su remisión a su correcto destinatario, procede señalar, sin embargo, que ello sólo implicó que la documentación correspondiente llegara finalmente a su destinatario correcto, pero no supuso una subsanación o una mitigación del impacto de la vulneración de la confidencialidad producida.

Segunda.- Falta de proporcionalidad en las sanciones impuestas

Alega el Ministerio que las sanciones propuestas no atienden al principio de proporcionalidad, al establecerse dos sanciones de apercibimiento, no concurriendo los requisitos de graduación de las sanciones establecidos en el apartado tercero del artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A este respecto, procede indicar que el artículo 77 de la LOPDGDD "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

Por tanto, siendo el Ministerio un responsable del tratamiento perteneciente a la Administración General del Estado le resulta de aplicación el precepto citado. Por tanto, en caso de infracciones al RGPD la sanción que corresponde imponer, por imperativo legal, es la de apercibimiento, no cabiendo otra y no siendo, por su propia naturaleza, susceptible de aplicar ningún criterio de graduación de los contenidos en el citado artículo 29 de la Ley 40/2015 ni de los establecidos por el RGPD o por la LOPDGDD.

Tercera.- Atipicidad de la conducta imputada

Sostiene en Ministerio que la descripción de los hechos y la calificación jurídica realizada no se subsume en ninguno de los supuestos definidos como infracción, invocando el artículo 25.1 de la Constitución Española, que exige que las conductas ilícitas -y las correspondientes sanciones- se encuentre predeterminadas normativamente, así como el artículo 27 de la Ley 40/2015, que recoge el principio de tipicidad. Arguye de nuevo que todo se debió a un error humano y que ello no supone que vulnere la confidencialidad ni que la brecha derive de una falta de medidas de seguridad adecuadas.

A este respecto, procede señalar que las infracciones en materia de protección de datos están tipificadas en los apartados 4, 5 y 6 del artículo 83 del RGPD. Es una tipificación por remisión, admitida plenamente por nuestro Tribunal Constitucional.

En este sentido, también el artículo 71 de la LOPDGDD realiza una referencia a las mismas al señalar que “Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.

En este sentido, el Dictamen del Consejo de Estado de 26 de octubre de 2017 relativo al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal dispone que “*El Reglamento Europeo sí tipifica, por más que lo haga en un sentido genérico, las conductas constitutivas de infracción: en efecto, los apartados 4, 5 y 6 de su artículo 83 arriba transcritos contienen un catálogo de infracciones por vulneración de los preceptos de la norma europea que en tales apartados se indican. El artículo 72 del Anteproyecto asume, no en vano, la existencia de dicho catálogo, cuando dispone que "constituyen infracciones los actos y conductas que supongan una vulneración del contenido de los apartados 4, 5 y 6 del Reglamento Europeo y de la presente ley orgánica*".

Las infracciones fijadas en los artículos 72, 73 y 74 del LOPDGDD lo son sólo a los efectos de la prescripción, tal y como reza el inicio de todos y cada uno de estos preceptos. Esta necesidad surgió en nuestro Estado dado que no existe en el RGPD referencia alguna a la prescripción relativa a las infracciones, dado que este instituto jurídico no es propio de todos los Estados miembros de la UE.

Debemos partir de que el RGPD es una norma jurídica directamente aplicable, que ha sido desarrollada por la LOPDGDD, sólo en aquello que le permite el primero. Así queda patente y en cuanto a la prescripción en la propia exposición de motivos de la LOPDGDD cuando expresa que “La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona”.

Por tanto, se cumple perfectamente el principio de tipicidad consagrado en nuestro ordenamiento jurídico, pues las conductas que se consideran ilícitas y sus correspondientes sanciones están perfectamente predeterminadas normativamente. Cuestión diferente es que el Ministerio no esté de acuerdo en que su conducta se considere que vulnera la normativa en materia de protección de datos, siendo subsumible en las infracciones imputadas, tal y como se ha motivado a lo largo del procedimiento sancionador y recogido en la presente Resolución.

Cuarta.- El Ministerio se reitera de todas las alegaciones hechas en anteriores escritos en el procedimiento sancionador.

A este respecto se indica que todas ellas ya fueron contestadas a lo largo de la tramitación del procediendo sancionador, estando recogidas en los Antecedentes de Hecho de la presente Resolución procediendo, por tanto, remitirse a las mismas.

Por todo lo expuesto, se desestiman las alegaciones aducidas.

IV
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*"

En el presente caso, consta que los datos personales del reclamante fueron indebidamente expuestos a un tercero (C.C.C.), (…), al habérsele enviado por correo electrónico un Oficio conteniendo información sobre circunstancias laborales de aquél (**...**).

Si bien no aparece directamente el nombre y apellidos del reclamante, resulta ser fácilmente identificable en dicho Oficio al hacerse mención en el mismo a un nombramiento suyo en el Boletín Oficial del Ayuntamiento de Madrid. Precisamente fue el C.C.C. quien informó al reclamante del envío erróneo al haberle podido identificar perfectamente por ese medio.

En este sentido, el artículo 4 del RGPD, en su apartado 1), define como *«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*

Por tanto, ello supone una comunicación no autorizada de datos personales a terceros.

A tenor de los hechos expuestos, se considera que corresponde imputar una sanción a la parte reclamada por la vulneración del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD.

V
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves"* de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

VI

Sanción por la infracción del artículo 5.1.f) del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la infracción del artículo 5.1.f) del RGPD, corresponde sancionar con un apercibimiento al Ministerio.

VII
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. 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, que en su caso incluya, entre otros:

> *a) la seudonimización y el cifrado de datos personales;*
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales*
> *de forma rápida en caso de incidente físico o técnico;*

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, en el momento de producirse la brecha, no cabe afirmar que la reclamada utilizase o contara con las medidas apropiadas para evitar el incidente y garantizar la confidencialidad, puesto que se remitió por correo electrónico a un tercero un Oficio de contestación de una solicitud formulada por el reclamante, lo que supuso una comunicación no autorizada de datos personales.

A tenor de los hechos expuestos, se considera que corresponde imputar una sanción a la parte reclamada por la vulneración del Artículo 32 del RGPD tipificada en el Artículo 83.4 del RGPD

VIII
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4,*

5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679. (…)*

IX

Sanción por la infracción del artículo 32 del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la infracción del artículo 32 del RGPD, corresponde sancionar con un apercibimiento al Ministerio.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES, con NIF S2801449F, por una infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD, una sanción de APERCIBIMIENTO.

SEGUNDO: IMPONER a MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES, con NIF S2801449F, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

TERCERO: NOTIFICAR la presente resolución a MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el

día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-010623

Mar España Martí
Directora de la Agencia Española de Protección de Datos