- **Expediente Nº: E/01778/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 28/10/2020, interpuso reclamación ante la Agencia Española de Protección de Datos (AEPD). La reclamación se dirige contra el SERVICIO PUBLICO DE EMPLEO ESTATAL con CIF Q2819009H (en adelante, SEPE). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante tuvo conocimiento de que sus datos de carácter personal estaban visibles para terceros en la página web del SEPE, a partir del 03/08/2020, ya que diferentes personas de toda España contactaron con ella a través de Internet, porque cuando intentaban realizar gestiones en relación al ERTE en el que estaban incursos, les aparecían los datos personales de la parte reclamante, nombre, dos apellidos, fecha de nacimiento y un nº asignado por la Administración (probablemente el número de la Seguridad Social), en lugar de los suyos propios.
Asimismo, manifiesta la parte reclamante que en su cuenta corriente bancaria se le efectuaron diferentes ingresos por valor de 3183´99 euros, que no le correspondían.

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), en fecha 27/11/2020 se dio traslado de dicha reclamación a la parte reclamada, 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.
No consta que el reclamado haya dado respuesta al traslado efectuado por la Agencia Española de Protección de Datos.

TERCERO: Con fecha 28/01/2021, se admitió a trámite la reclamación presentada por la parte reclamante, al amparo de lo establecido en el artículo 65.5 de la LOPDGDD.

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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

La reclamante pone de manifiesto los siguientes hechos:

- En su escrito del 28 de octubre señala que, desde el 1 de agosto sus datos personales son mostrados a terceros en la sede electrónica del reclamado cuando estos terceros acceden a consultar sus prestaciones. En su escrito del 19 de noviembre refiere el día 3 de agosto como la fecha en la que tuvo conocimiento de que esta situación se estaba produciendo. Asimismo señala que los datos personales de la reclamante a disposición de los terceros eran: ***(…).***
- En su escrito del 28 de octubre declara haber puesto los hechos en conocimiento del reclamado hasta en dos ocasiones sin que la situación haya sido rectificada. Asimismo manifiesta haber interpuesto denuncia ante *"las autoridades competentes".*
- En su escrito del 19 de noviembre manifiesta que el reclamado le realizó el 5 de octubre doce ingresos por error a nombre de otros tantos beneficiarios de la prestación. Ante esta situación solicitó por escrito al reclamado una aclaración con respecto al motivo de los ingresos y el procedimiento de devolución (señala que pudo devolver el dinero y que "han admitido que se debe a un gran error desde la Subdirectora Provincial de Prestaciones del SEPE en ******PROVINCIA.1***)** y que se informe de la situación al Delegado de Protección de Datos del reclamado (declara no haber recibido respuesta en relación con este punto)

Documentación relevante aportada por el reclamante:

- Certificado de realización de denuncia presentada por revelación de secretos el día 7 de agosto de 2020 en la "******COMISARÍA.1***" de ******LOCALIDAD.1***. En la denuncia refiere la reclamante que tomo consciencia de la situación el 1 de agosto de 2020 cuando *"comenzó a recibir mensajes en el Messenger de Facebook, en el que personas de diferentes lugares de España se ponían en contacto con la denunciante para informarle que en la página oficial del SEPE, cuando introducía su D.N.I para solicitar algún tipo de prestación figuraba* ***(…)*** *de la dicente."*
- Certificado de realización de ampliación de la denuncia el día 21 de agosto de 2020 en la "******COMISARÍA.1***" de ******LOCALIDAD.1***. La reclamante manifiesta que *"los hechos denunciados se han seguido produciendo".*
- Escrito dirigido al Delegado de Protección de Datos del reclamado fechado el 13 de octubre de 2020 en el que se alega la recepción de diversos ingresos procedentes del reclamado el día 5 de octubre y se solicita aclaración e indicación de la vía para proceder a su devolución. Adjunta justificante de registro del escrito el 14 de octubre de 2020.
- Escrito dirigido al Delegado de Protección de Datos del reclamado fechado el 13 de octubre de 2020 en el que se alega haber tenido conocimiento de que sus datos personales han estado accesibles para terceros a través del **"*(…)*"** y solicita la retirada inmediata de los mismos. Adjunta justificante de registro del escrito el 14 de octubre de 2020.
- Un conjunto de impresiones de pantalla del teléfono móvil (págs. 10 a 83 del documento anexo al escrito) que muestran conversaciones en las que diferentes personas se comunican con la reclamante

comunicándole el acceso a sus datos personales a través de la sede del reclamado. Los terceros le comunican que***(…).***

- Impresiones de pantalla que muestran los ingresos realizados en la cuenta de la reclamante con fecha de 5 de octubre de 2020 y las devoluciones de los mismos (págs. 84 a 92 del documento anexo al escrito).

Los antecedentes que constan en los sistemas de información son los siguientes:
En el marco del procedimiento E/09572/2020, con fecha de 27 de noviembre de 2020 la AEPD, en virtud del artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales , dio traslado de la reclamación al reclamado a través de medios electrónicos (notificación electrónica). El servicio de Soporte del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada certificó posteriormente el rechazo automático de la misma tras haber transcurrido diez días naturales desde su puesta a disposición.

Cronología de hechos. Causas y medidas de resolución de la brecha de seguridad:
En relación con los hechos acontecidos el reclamado en su escrito manifiesta que durante el mes de agosto de 2020 ***(…).***
Adjunta, copia ***(…).*** Éste apunta que 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 derivado de una competencia atribuida por una norma con rango de ley (Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social).
(…). Así, señala que el 26 de agosto de 2020 la incidencia quedó resuelta.

Resume las medidas tomadas para la resolución en los siguientes puntos:

- ***(…).***

Tipología de datos personales y número de afectados.
Añade el reclamado que la tipología de datos personales afectados es de carácter básico ***(…).***
La reclamante, tal y como se ha visto anteriormente, refiere en la reclamación que los datos personales afectados por la brecha de seguridad habrían sido: ***(…)****.*

Análisis de riesgos, Evaluación de Impacto, y medidas de seguridad
El escrito incluye la Orden de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social. El primer artículo de la orden señala que *"tiene por objeto aprobar la política de seguridad que proteja adecuadamente todos los SSII del Ministerio de Empleo y Seguridad Social y garantice que prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas."* Asimismo el artículo undécimo, titulado *"Normativa de seguridad"* postula una organización en cuatro niveles (los tres primeros obligatorios y el cuarto opcional): política de seguridad, normas de seguridad, procedimientos de seguridad, y un cuarto nivel que refiere como *"documentación de buenas prácticas, recomendaciones, etc."*
El propio apartado 4.4 incorpora también la Instrucción de la Dirección General del Servicio Público de Empleo Estatal por la que se aprueba la Organización de la Seguridad de la Información en el ámbito de la administración electrónica del

Organismo firmada el 12 de febrero de 2013 y realizada de conformidad con la citada orden.
En cuanto a la gestión de los incidentes de seguridad, el escrito incorpora la norma de gestión de incidentes de seguridad aprobada el 27 de noviembre de 2018 clasificada como de *"DIFUSIÓN LIMITADA"*. El objeto de la norma, según se informa en la misma, es ***"(…)."*** El apartado cuarto de la norma incluye los roles y responsabilidades de los distintos actores, ***(…)***. Igualmente señala a la AEPD como la entidad a la que han de notificarse incidentes de seguridad que involucren datos de carácter personal. El apartado quinto de la norma, relativo a la gestión de incidentes de seguridad, incluye, entre otras, las siguientes pautas de actuación:
"(…)".

En relación con la información general en materia de seguridad de los sistemas de información, el escrito incorpora en el apartado 4.6 el documento *"Procedimiento Planificación y Seguimiento de Inspecciones TIC de Seguridad (SGTIC). Gestión de Seguridad de los Sistemas de Información"* de agosto de 2020 cuyo objeto es *"definir las pautas de actuación para la gestión de inspecciones TIC de seguridad, así como identificar los roles y responsabilidades de los involucrados".*
Ya en relación con el tratamiento concreto afectado por la brecha de seguridad, el registro de actividad incorporado en el apartado 4.1 del escrito incluye un apartado titulado *"ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO"* del cual se subraya lo siguiente:

- ***"(…)***
- ***(…)***
- ***(…)".***

Además de las anteriores este apartado incluye un total de nueve bloques con un total de veintiocho cuestiones en formato pregunta/respuesta binaria "Sí/No" sobre los siguientes temas: ***"(…)".***
El registro de actividad concluye del análisis de riesgos anterior que las medidas adoptadas para este tratamiento se corresponden con ***(…)***. Además recomienda la adopción de las siguientes acciones:

1. ***"(…)***
2. ***(…)***
3. ***(…)"***

Adjunta copia del documento *"ANÁLISIS DE RIESGOS AÑO 2020 SERVICIOS CENTRALES – SGPD"* realizado, según informa en el propio escrito,***(…)***. La versión facilitada del documento, de siete páginas, incluye los apartados introducción y resumen ejecutivo. Se cita como objeto del mismo recoger *"los resultados del análisis de riesgos de seguridad de la información, realizado en el Año 2020, correspondiente a la Subdirección General de Prestaciones por Desempleo"* y expresa que su ejecución responde al *"requisito recogido en el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica".* El análisis abarca tres sistemas de información,***(…)***.
Los apartados 4.3 y 5 del escrito listan las medidas implantadas (correspondientes a las
(…).

Respecto de la notificación de la brecha de seguridad a la AEPD.

No existe constancia de recepción de la notificación de la violación de seguridad de datos personales a la AEPD en relación con los hechos aquí investigados.
No obstante, el registro de actividad facilitado incluye respuestas afirmativas a las siguientes cuestiones:

- *"¿Se notifican a la Agencia Española de Protección de Datos, sin dilación indebida, las violaciones de la seguridad de los datos personales que constituyan un riesgo para los derechos y libertades de las personas físicas?"*
- *"¿Se notifican a los interesados, sin dilación indebida, las violaciones de la seguridad de los datos personales que entrañen un alto riesgo para sus derechos y libertades?"*

En relación con la notificación a los interesados el reclamado expresa que no se ha realizado comunicación al respecto ya que *"puede provocar falsa alarma social".*

En relación con la potencial utilización de los datos personales afectados por la brecha de confidencialidad manifiesta el reclamado que no tiene constancia de la explotación o uso de los datos de la reclamante por parte de terceros al no tener esta circunstancia *"un impacto directo en los sistemas del SEPE"*.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra 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."*
El artículo 5 apartado 1 f) del RGPD establece que "*Los datos personales serán 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»)".*

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto 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.

Artículo 32

"Seguridad del tratamiento

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".

Artículo 33

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la

seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a)describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b)comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c)describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d)describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Artículo 34:

"Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la segu-

ridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

III

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, al haber tenido acceso a datos personales de la parte reclamante personas no autorizadas a ello.

De la documentación obrante en el expediente y de las investigaciones llevadas a cabo, se desprende que se han vulnerado los citados artículos 5.1.f), 32 y 33 del RGPD, por lo que correspondería iniciar un Procedimiento Sancionador contra el SEPE.

No obstante, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) recoge el principio NON BIS IN IDEM, al establecer en su artículo 31.1:

"No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento".

Consultados los antecedentes que obran en la AEPD, consta Procedimiento Sancionador PS/00203/2021, finalizado con resolución sancionadora notificada el 28/09/2021, en el que coinciden, con respecto al presente procedimiento, el sujeto, el hecho y el fundamento jurídico.

IV

De conformidad con lo indicado en los párrafos anteriores y con la información de la que se dispone en este momento, aún habiendo evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos, por aplicación del citado principio “NON BIS IN IDEM” se concluye que no procede iniciar un nuevo Procedimiento Sancionador.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***A.A.A.*** y SERVICIO PUBLICO DE EMPLEO ESTATAL, con CIF Q2819009H.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

940-051121

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