Expediente nº.: EXP202306260

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por **THE PHONE HOUSE SPAIN, S.L.** (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 27 de diciembre de 2023, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 27 de diciembre de 2023, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202306260, en virtud de la cual se imponía a **THE PHONE HOUSE SPAIN, S.L.** (TPHS) con NIF B81846206

- por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una multa administrativa de 4.000.000 € (cuatro millones de euros).

- por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD, una multa administrativa de 2.500.000,00 € (dos millones quinientos mil euros).

Dicha resolución, que fue notificada a la parte recurrente en fecha 27 de diciembre de 2023, fue dictada previa tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00084/2023, quedó constancia de los siguientes:

HECHOS PROBADOS

PRIMERO: Primera notificación de la brecha de datos personales

Con fecha 14 de abril de 2021, TPHS notifica a la AEPD una brecha de datos personales indicando en el "*Informe de incidente de seguridad*" que adjunta que se trata de:

> ***(…).***
>
> (…) *Actualmente se está investigando el alcance de la incidencia y a fecha de hoy no se tiene constancia de que se haya tenido acceso a datos de carácter personal*

(…) Se están realizando investigaciones, así como un análisis forense del ataque y del modo de acción de los atacantes.

(…) Se han contratado los servicios de la empresa especializada en ciberseguridad, SIA GROUP, para analizar y gestionar la crisis originada por la incidencia de seguridad".

SEGUNDO: Segunda notificación de la brecha de datos personales

Con fecha 28 de abril de 2021 TPHS presenta una nueva notificación ampliando la información sobre la brecha de datos personales notificada, a través de la aportación de un "*Informe de evaluación de brecha de seguridad*", fechado el 28 de abril de 2021, según el cual:

- "*Se ha podido evidenciar que los atacantes habían descargado durante el ataque información que contenía datos personales.*

(…) *El ataque comprometió la confidencialidad (…) Dicho proceso se habría producido mediante exportaciones no legítimas realizadas por el atacante de la base de datos en producción de clientes, antiguos clientes, proveedores y empleados de Phone House por parte de terceros no autorizados*"

(…).

TERCERO: Cronología del ataque

Según "*Informe de evaluación de brecha de seguridad*", fechado el 28 de abril de 2021, aportado por TPHS junto con la segunda notificación de brecha de datos personales presentada el 28 de abril de 2021, la cronología del ataque es la siguiente:

-Fecha inicio del ataque: 31 de marzo de 2021 (estimado): ***(…).***
-Fecha de detección: 11 de abril de 2021
-Fecha de resolución: 21 de abril de 2021

CUARTO:

En el "*Informe de análisis de incidente ransomware*" elaborado por la empresa SIA Group, contratada tras el incidente por TPHS para el análisis de lo ocurrido y fechado el 21 de abril de 2021, y aportado por TPHS EL 1 de marzo de 2021 ***(***Número de registro: ******REGISTRO.1***) se pone de manifiesto lo siguiente:

(…).

QUINTO: Número de personas afectadas:

En el "Informe de Evaluación de Brecha de Seguridad", fechado el 28 de abril de 2021, indica TPHS *"Número aproximado de personas afectadas:13.000.000".*

SEXTO: Tipos de datos afectados:

Indica TPHS en su "*Informe de evaluación de brecha de seguridad*", fechado el 28 de abril de 2021,

"*Con respecto a los datos afectados por la brecha de confidencialidad pueden diferenciarse cuatro categorías de datos afectadas*:

Empleados:

-Datos identificativos básicos: nombre, apellidos, DNI o documento identificativo equivalente.
-Datos de detalles de empleo y datos de contacto profesional: Puesto, número de empleado, ciudad, fecha de incorporación a la compañía y correo electrónico empresarial.

Proveedores:

-Datos identificativos básicos: nombre y apellidos
-Datos de contacto profesional: correo electrónico empresarial.

Clientes y antiguos clientes:

-Datos identificativos básicos: nombre, apellidos, nombre de usuario, DNI o documento identificativo equivalente.
-Datos de contacto: teléfono, dirección postal, correo electrónico.
-Fecha de nacimiento, género y nacionalidad.
-Número de cuenta bancaria de aquellos clientes que hayan contratado un seguro.
-Información relativa a los productos adquiridos o servicios contratados."

En "Informe de análisis de incidente ransomware" elaborado por la empresa SIA Group, fechado el 21 de abril de 2021, se añade también el siguiente dato personal:

-Número de IMEI de teléfono

SÉPTIMO: Publicación de los datos personales en la Deep Web por los ciberatacantes:

En el "Informe de evaluación de brecha de seguridad", fechado el 28 de abril de 2021, aportado por TPHS junto con la segunda notificación de brecha de datos personales presentada el 28 de abril de 2021, TPHS manifiesta:

(…).

En el "*Informe de análisis de incidente ransomware*" elaborado por la empresa SIA Group, contratada tras el incidente por TPHS para el análisis de lo ocurrido y fechado el 21 de abril de 2021, y aportado por TPHS EL 1 de marzo de 2021 (Número de registro: ******REGISTRO.2***) se indica:

(…).

OCTAVO:

Los datos personales publicados en la Deep Web por el/os ciberatacante/s de los clientes de TPHS aparecen en texto claro.

NOVENO: En relación con la política de contraseñas:

En el "*Informe de análisis de incidente ransomware*" elaborado por la empresa SIA Group, contratada por TPHS con posterioridad a la brecha de datos personales y para el de ésta y fechado el 21 de abril de 2021, se indica:

(…).

El inventario de sistemas aportado por TPHS el 28 de junio de 2021 (Número de registro: O00007128e2100028705), en relación con las medidas de control de acceso lógico a los sistemas de información, contiene la siguiente información relevante:

(…).

En el Informe "*Evaluación del cumplimiento en materia de protección de datos – Medidas de Seguridad –*", realizado por un tercero (Écija) y fechado el 11 de enero de 2021 (poco más de dos meses antes del incidente), aportado por TPHS el 17 de agosto de 2022 (Número de registro: REGAGE22e00035656325) en el que se realiza un análisis de las obligaciones en materia de seguridad y organizativas de TPHS conforme a la normativa en materia de protección de datos personales, concretamente de las medidas de seguridad técnicas, se pone de manifiesto lo siguiente:

(…).

DÉCIMO: Guía CCN-STIC-807

La Guía CCN-STIC-807, publicada en marzo de 2011 por el Centro Criptológico Nacional (CCN), ***(…).***

DÉCIMO PRIMERO: En relación con la protección de la seguridad perimetral de los sistemas de información y de las medidas de monitorización para la detección de conducta maliciosa dentro de la red.

En el "*Informe de análisis de incidente de ransomware*" realizado por la empresa SIA Group, fechado el 21 de abril de 2021 se indica lo siguiente:

(…).

DÉCIMO SEGUNDO: Medidas adoptadas por TPHS con posterioridad al incidente:

1. En el documento sobre "*Procedimiento de gestión de usuarios y contraseñas*" (versión 4.0 vigente desde el 3 de mayo de 2021) aportado por TPHS el 11 de marzo de 2022 (Número de registro: REGAGE22e00006497111) se incluyen las siguientes medidas que no constaban en la anterior versión 3.0 que estaba vigente en el momento de la brecha de datos personales (y aportada por TPHS con el mismo número de registro cuya última actualización indica el 29/09/2020):

(…).

2. TPHS indica en su "*Informe de evaluación de brecha de seguridad*", fechado el 28 de abril de 2021 y presentado junto a la segunda notificación de brecha presentada el mismo día, las siguientes "*Medidas mitigadoras adoptadas desde el incidente*":

(…).

En el mismo informe indica como "*Medidas en proceso de implantación*":

(…).

DÉCIMO TERCERO:

En el marco de las actuaciones previas de investigación, mediante escrito de 8 de julio de 2022, esta Agencia requirió a TPHS lo siguiente:

"En las EIPD relativas a las actividades de tratamiento "Marketing digital", "Comunicaciones comerciales" y "Control de Acceso a las Instalaciones" se concluye un riesgo residual al tiempo que se determinan un conjunto de medidas de seguridad al objeto de reducirlos riesgos detectados. A este respecto se requieren:

i. Evidencias de la implantación/ejecución, antes del incidente, de las medidas establecidas en dichas EIPDs para mitigar los riesgos tipificados como "altos" o "muy altos" detectados.

ii. En particular, evidencias de la adopción antes del incidente, de las siguientes medidas dirigidas a mitigar el riesgo "muy alto "derivado del tratamiento masivo y a gran escala o de la observación sistemática y que se indican en la propias EIPDs:

- (…)
- Implementar medidas de seudonimización y anonimización para el tratamiento de datos personales.
- Implementar medidas de seudonimización y anonimización suficientes (k anonimización) en el caso de tratamiento de datos especialmente masivos.
- Limitar el acceso a dicha información a las personas que tengan que acceder necesariamente a dichos datos
- Informar de manera transparente de las finalidades del tratamiento.

Mediante escrito presentado por TPHS el 17 de agosto de 2022 (número de registro: REGAGE22e00035653351), responde lo siguiente:

"En el informe aportado al presente escrito como Documento nº 2, que contiene la evaluación de cumplimiento del RGPD y la LOPDGDD desde un punto de vista jurídico organizativo, se analizó el cumplimiento del principio de transparencia, el cual denotó un cumplimiento generalizado de las cuestiones examinadas, sin perjuicio de la identificación de aspectos de mejora tal y como se refleja en el citado Documento.

Sobre la limitación del acceso a la información, tal y como está indicado en el documento nº 1 (apartado 5.1 y 6.4) PHONE HOUSE había (y continúa

haciéndolo) implementado un sistema efectivo de gestión de usuarios por roles y permisos que hace que cada empleado sólo acceda a la información que es necesaria para realizar sus labores profesionales.

Tal y como se aporta en el documento nº 1, PHONE HOUSE había implantado en los sistemas que técnica y organizativamente era aplicable, medidas relacionadas con la seudonimización, anonimización y en su caso bloqueo (apartado 6.16 del documento)"

Los documentos nº 1 y nº 2 a los que se refiere TPHS son, respectivamente los informes "*Evaluación del cumplimiento en materia de protección de datos – Medidas de Seguridad –*", realizado por un tercero (Écija), aportado por TPHS el 17 de agosto de 2022 (Número de registro: REGAGE22e00035656325) y "*Evaluación del cumplimiento en materia de protección de datos - aspectos jurídico-organizativos –*" fechado el 11 de enero de 2021 y aportados por TPHS el 17 de agosto de 2022 (Número de registro: REGAGE22e00035663361).

DÉCIMO CUARTO: Evaluaciones de Impacto de Protección de Datos: Evaluación del riesgo

En las EIPD realizadas por TPHS respecto de las actividades de tratamiento afectadas por la brecha de datos personales ("Marketing", "Comunicaciones comerciales" "Control de acceso a las instalaciones"), fechadas en 2018 y aportadas por TPHS el 28 de junio de 2022 (número de registro: O00007128e2100028701), se realiza una descripción de las siguientes "amenazas", se valora el "riesgo" y se indican las "medidas" para mitigar esos riesgos (a modo de ejemplo y sin carácter taxativo):

Respecto de la actividad de tratamiento "Comunicaciones comerciales":

AMENAZA	Se tratan datos de orígenes desconocidos o de fuentes no aptas para el tratamiento.	Alto
MEDIDAS	Revisar la información recogida para evitar recoger datos personales de fuentes desconocidas. • Regularizar contractualmente la relación con los terceros que aporten los datos. • Establecer un procedimiento de gestión de recogida de la información (fuentes confiables). • Exigir contractualmente la regularización en origen del tratamiento de datos. • Exigir contractualmente la realización de controles periódicos para verificar el cumplimiento normativo.	

AMENAZA	La información facilitada en entornos específicos (web, app, formularios) no cumple con los requerimientos específicos que puedan afectar a su soporte	Alto

MEDIDAS	• Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada. • Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. • Verificar que la información que se ofrece con total claridad en todas las ubicaciones, funcionalidades y formularios en los que se recaben datos personales, y que la misma es coherente y sistemática. • Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. • Adoptar los textos legales al soporte en el que se facilita la información a los interesados. • En el caso de información sobre cookies, implantar un sistema adecuado a la navegación que permita la información por capas. • En el caso de aplicaciones móviles, facilitar las políticas tanto en la propia aplicación como en la tienda de aplicaciones pertinente.

AMENAZA	**Se tratan datos personales para el envío de comunicaciones comerciales sin la legitimación adecuada.**	**Alto**
MEDIDAS	• Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales para el envío de comunicaciones comerciales. • Si el tratamiento está legitimado con base al interés legítimo de responsable verificar que el tratamiento cumple con los requisitos legales. • Si el tratamiento está basado en interés legítimo verificar que la base de datos es propia y no de terceros. • Si el tratamiento de datos está basado en la excepción de la LSS verificar que las comunicaciones se realizan a sujetos que ya son clientes de la empresa, las comunicaciones son de la misma empresa que han contratado y que los productos o servicios son similares. • Implementar un sistema interno para facilitar la baja de comunicaciones comerciales de manera automática	

AMENAZA	**No se han revisado adecuadamente las medidas de seguridad que ofrece un Encargado de Tratamiento**	**Alto**
MEDIDAS	• Establecer procedimientos y mecanismos que permitan evaluar, previamente a la contratación, la adecuación de los distintos proveedores que podrían actuar como encargados de tratamiento. • Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros.	

AMENAZA	**Realización de perfilados con motivos de marketing o analítica de manera inadecuada o sin cumplir con los requisitos legales**	**Alto**
MEDIDAS	• Recabar el consentimiento inequívoco de los interesados. • Si el tratamiento está basado en un interés legítimo, se han ponderar los intereses del responsable frente a los de los interesados. • Realizar el tratamiento con datos internos y no acudir a bases externar no legitimadas. • Si se realiza el tratamiento contra una base de datos externa, se ha regularizado contractualmente dicho tratamiento de datos. • Se pone a disposición del interesado una opción para oponerse a la realización de este tratamiento. • Se informa claramente del tratamiento realizado, así como de la lógica utilizada para este tratamiento.	

Respecto a la actividad de tratamiento “Marketing digital":

AMENAZA	**Cuando los datos son obtenidos directamente de los interesados, no se les informa conforme a los requisitos establecidos en el artículo 13 del RGPD.**	**Alto**
MEDIDAS	• Establecer un procedimiento que garantice que las obligaciones asumidas en los contratos suscritos y/o en las condiciones de uso dispuestas son validadas por asesoría jurídica, garantizándose su cumplimiento a nivel corporativo. • Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada. • Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. • Verificar que la información que se ofrece con total claridad en todas las ubicaciones, funcionalidades y formularios en los que se recaben datos personales, y que la misma es coherente y sistemática. • Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.	

AMENAZA	**Realización de perfilados con motivos de marketing o analítica de manera inadecuada o sin cumplir con los requisitos legales**	**Alto**
MEDIDAS	• Recabar el consentimiento inequívoco de los interesados Si el tratamiento está basado en un interés legítimo, se han ponderar los intereses del responsable frente a los de los interesados. • Realizar el tratamiento con datos internos y no acudir a bases externar no legitimadas. • Si se realiza el tratamiento contra una base de datos externa, se ha regularizado contractualmente dicho tratamiento de datos.	

		RIESGO
AMENAZA	**El sujeto no es consciente claramente del profiling/scoring realizado**	**Alto**
MEDIDAS	• Se pone a disposición del interesado una opción para oponerse a la realización de este tratamiento. • Se informa claramente del tratamiento realizado, así como de la lógica utilizada para este tratamiento. • Recabar el consentimiento inequívoco de los interesados. • Si el tratamiento está basado en un interés legítimo, se han ponderar los intereses del responsable frente a los de los interesados.	
		RIESGO
AMENAZA	**No se tiene en cuenta la privacidad en el diseño de nuevas operaciones de tratamiento, desarrollos o funcionalidades informáticas, productos y/o servicios**	**Alto**
MEDIDAS	• Establecer procedimientos para el diseño de nuevas operaciones de tratamiento, desarrollos o funcionalidades informáticas, productos y/o servicios (Privacy by Design). • Incluir en los procedimientos de Privacy by Design la incorporación, entre otros, del DPO en las fases iniciales de los mismos. • Establecer y definir claramente desde la dirección las funciones, competencias y atribuciones del DPO en el desarrollo y gestión de los proyectos.	

DÉCIMO SEXTO: Tratamientos de datos personales que incluyen la realización de perfiles (*profiling*)

En el documento donde se recoge el Registro de Actividades de Tratamiento y análisis de riesgos, aportado por TPHS el 28 de junio de 2022 (número de registro: ******REGISTRO.3***), se indica:

Respecto de la actividad “Marketing Digital”:

-“Tratamientos a gran escala: SÍ
- Scoring/profiling: SÍ”

Respecto de la actividad de tratamiento “Comunicaciones comerciales”:

- *“Tratamientos a gran escala: SÍ*
- *Scoring/profiling: SÍ*”

En el Registro de Actividades de Tratamiento, aportado por TPHS en fecha 15 de septiembre de 2023 (Número de registro: REGAGE23e00062166595), en respuesta al requerimiento efectuado por esta Agencia en el trámite de práctica de prueba, se indica

Respecto de la actividad de tratamiento “Elaboración de perfiles”:

“-Finalidades del tratamiento: Elaboración de perfiles a fin de realizar publicidad personalizada.
-Categoría de datos: (i) Datos identificativos: Nombre y apellidos; (ii) Datos de contacto: correo electrónico, dirección postal y teléfono; (iii) Datos sobre los servicios o productos contratados: servicio o producto; (iv) Datos obtenidos a través de los contenidos generados por los usuarios: comentarios, mensajes privados o chat u otros elementos virtuales.
-Categoría de interesados: i) Clientes; (ii) Potenciales clientes; (iii) Usuarios web”

DÉCIMO SÉPTIMO: Cursos de formación

1. En contestación a requerimiento de información por parte de esta Agencia, TPHS presenta, el 17 de agosto de 2022, (Número de registro: REGAGE22e00035653351) escrito en el que manifiesta:

“*PHONE HOUSE cuenta con un plan de formación que tiene como principal objetivo mantener los conocimientos de sus trabajadores debidamente actualizados ayudándolos al desarrollo de nuevas competencias y la mejora de las ya existentes.*

En materia de protección de datos se han impartido distintos cursos y formaciones que abarcan tanto un enfoque general de la materia, como el desarrollo de cuestiones más específicas que se han detectado en la Compañía como especialmente relevantes, debido al impacto que tienen en sus empleados y clientes.

En este sentido, PHONE HOUSE impartió cursos centrados en la seguridad de la información y la protección de datos, tanto con carácter previo a la plena aplicación del RGPD, con en el momento de su adaptación a la, en aquel entonces nueva norma europea, año 2018. Se acompaña como Documento nº 3 e listado de asistentes a las formaciones y el detalle de éstas.

Se acompaña como documento nº 4, evaluación y conocimientos tipo test que deben realizar después de recibir la formación en materia de protección de datos, los trabajadores, en el momento de incorporarse a la Compañía.

Adicionalmente PHONE HOUSE cuenta con una Política de Seguridad de la Información, la cual se acompaña como Documento nº 5.”

Adjunta al escrito anterior la siguiente documentación (Número de registro: REGAGE22e00035656325):

- Documento 3. "*Programa formativo PROG-294. Nombre del programa: Reglamento Europeo de Protección de Datos"*

Es un listado de participantes en dos cursos sobre el "Reglamento Europeo de Protección de Datos" abiertos entre mayo de 2018 y diciembre de 2020. En el primero de los cursos hay 388 inscritos. En el segundo hay inscritos 254.

- Documento 4. Recoge preguntas tipo test

- Documento 5. Política de Seguridad de la Información, versión 2, de marzo de 2022.

2. TPHS, en su escrito de alegaciones al Acuerdo de Inicio, presentado el 29 de marzo de 2023, en fecha 15 de septiembre de 2023 (Número de registro: ******REGISTRO.4***), indica:

"*1) En el año 2015, con carácter previo a la entrada en vigor del RGPD, los trabajadores de PHONE HOUSE recibieron una formación presencial en sus oficinas por parte de* ***A.A.A.****, catedrático de Universidad y socio del despacho de abogados* ***A.A.A..*** *Se acompaña como documento nº4 el contenido de la formación y documentos utilizados por el Sr.* ***A.A.A.*** *en el año 2015.*

2) Entre el año 2015 y el año 2016 los trabajadores de PHONSE HOUSE realizaron un curso de formación en materia de protección de datos a través de la plataforma E-learning. En la captura de pantalla que se acompaña a continuación queda evidenciado que, en fecha 17 de noviembre de 2015, se remitió un correo electrónico a los trabajadores indicándoles que debían realizar la formación en materia de protección de datos.

6) *En el año 2017, PHONE HOUSE lanzó en su plataforma online un nuevo curso para todos sus trabajadores cuyo contenido se acompaña como documento nº5.*

2) En el año 2018, en el momento en que resultó plenamente aplicable el RGPD, el despacho de abogados ECIJA realizó varias formaciones presenciales en las oficinas de PHONE HOUSE. Se acompaña como documento nº6 el contenido del curso impartido en 2018 por ECIJA.

3) Adicionalmente, a partir del 24 de mayo del año 2018, todos los trabajadores de PHONE HOUSE debían realizar el curso online, sobre protección de datos y seguridad de la información, disponible en la plataforma online Dominion University: https://iseazy.com/dl/ff8e1eff94d54d4885fb82698c0a4fbc. Este curso también lo realizaron todos los trabajadores contratados con posterioridad a 2018, en el momento de incorporarse a la Compañía.

4) Entre el 7 de abril del año 2020 y el 30 de agosto de 2020 se activó un nuevo curso de formación para aquellos trabajadores que iban a gestionar seguros de Liberty, en los que PHONE HOUSE ostenta el rol de mediador. A continuación, se incluye captura de pantalla a fin de evidenciar que el citado curso estaba disponible para los trabajadores que gestionaban seguros en la Intranet de PHONE HOUSE:

5) En el año 2021, atendiendo al principio de accountability, que caracteriza las actuaciones de PHONE HOUSE en todo momento, se actualizó el contenido del curso que debían realizar todos los trabajadores por el siguiente: ******URL.1.***

6) En el año 2022, se actualizó de nuevo el contenido del curso en materia de protección de datos y seguridad de la información, incluyendo al final de la formación un examen tipo test que tienen que realizar todos los trabajadores al finalizar el mismo. A continuación, se incluye captura de pantalla conforme se evidencia que el curso está disponible en la intranet de PHONE HOUSE."

Junto al escrito de alegaciones al Acuerdo de Inicio, presentado en fecha 29 de marzo de 2023, TPHS aporta los siguientes documentos relativos a los cursos indicados anteriormente:

"Documento nº4: Contenido de la formación y documentos utilizados por ***A.A.A.*** *en el año 2015.*

Documento nº5: Contenido de la formación ofrecida por PHONE HOUSE a sus trabajadores en el año 2017.

Documento nº6: Contenido de la formación impartida en el año 2018.

Documentos nº7, 8, 9 y 10: Algunos de los listados de las formaciones realizadas por los trabajadores en materia de protección de datos."

DÉCIMO OCTAVO: Según la información obtenida del servicio Axesor (ver Diligencia Referencias), TPHS cuenta con 1.411 empleados en el ejercicio 2020.

DÉCIMO QUINTO: Evaluaciones de Impacto de Protección de Datos: Medidas.

En las EIPD realizadas por TPHS respecto de las actividades de tratamiento afectadas por la brecha de datos personales ("Marketing", "Comunicaciones comerciales" "Control de acceso a las instalaciones"), fechadas en 2018, dos años antes de la brecha de datos personales, y aportadas por TPHS el 28 de junio de 2022 (número de registro: O00007128e2100028701) en las que se detectan riesgos "altos" o "muy altos" y, en consecuencia, se determinan una serie de medidas a adoptar al objeto de mitigar esos riesgos.

Entre ellas se señalan las siguientes:

(…).

DECIMO SEXTO:
En el Informe “Evaluación del cumplimiento en materia de protección de datos – Medidas de Seguridad –“, fechado el 11 de enero de 2021, se pone de manifiesto lo siguiente:

(…).

DÉCIMO SÉPTIMO: Registro de Actividades del tratamiento

El en Registro de Actividades de Tratamiento de TPHS, aportado por ella en fecha 15 de septiembre de 2023, en respuesta al requerimiento efectuado por esta Agencia en el trámite de práctica de prueba, aparece la actividad de tratamiento “Elaboración de perfiles”, respecto de la que se indica:

> *“-Finalidades del tratamiento: Elaboración de perfiles a fin de realizar publicidad personalizada.*
> *-Categoría de datos: (i) Datos identificativos: Nombre y apellidos; (ii) Datos de contacto: correo electrónico, dirección postal y teléfono; (iii) Datos sobre los servicios o productos contratados: servicio o producto; (iv) Datos obtenidos a través de los contenidos generados por los usuarios: comentarios, mensajes privados o chat u otros elementos virtuales.*
> *-Categoría de interesados: i) Clientes; (ii) Potenciales clientes; (iii) Usuarios web*”.

TERCERO: La parte recurrente ha presentado en fecha 29 de enero de 2024, en esta Agencia Española de Protección de Datos, recurso de reposición, fundamentándolo, básicamente, en las siguientes alegaciones:

PRIMERA- SOBRE LA FALTA DE MOTIVACIÓN DE LA PROPUESTA RESOLUCIÓN

Considera la parte recurrente que la resolución dictada por la AEPD no está debidamente motivada y que ha eludido contestar alegaciones como las referidas a la coincidencia de las medidas técnicas y organizativas apropiadas requeridas por los artículos 5.1 f) y 32 del RGPD. Entiende a este respecto que la consideración de obligaciones distintas no ha sido debidamente justificada. Considera la parte recurrente que la resolución recurrida no responde a la exigencia de motivación de las resoluciones administrativas exigidas tanto por la jurisprudencia del Tribunal Supremo como por el Tribunal Constitucional.

SEGUNDA. - CONDICIÓN DE VÍCTIMA DE PHONE HOUSE

Entiende la recurrente que la resolución del expediente sancionador ha de tener en cuenta el origen delictivo de los hechos. Y que, debido a las características del ciberataque del que fue víctima, no existían medios para prevenirlo o revertirlo, a pesar de las medidas de seguridad adoptadas.
Considera que durante la tramitación del expediente sancionador se realizaron alegaciones tendentes a demostrar la inversión realizadas en servicios de seguridad antes de la brecha de datos personales y con posterioridad a la misma. Asimismo,

considera incorrecta la mención realizada en la resolución recurrida a los efectos de la brecha en el derecho a la protección de datos personales de los afectados, puesto que entiende que esta seguridad es ampliamente tenida en cuenta por la recurrente, que también ha de considerarse como víctima y, por lo tanto, afectada, por la brecha acaecida.

TERCERA. – SOBRE EL SUPUESTO INCUMPLIMIENTO DEL ARTÍCULO 5.1.F) RGPD

En este punto, la recurrente se remite a las alegaciones ya realizadas al afecto durante la tramitación del procedimiento sancionador e insiste en que actuó en todo momento de forma diligente, con medidas de seguridad adecuadas y razonables en atención al riesgo asociado al tratamiento de datos realizado y en los sistemas de información afectados por la brecha.

Recuerda expedientes previos tramitados por la AEPD, concluidos con el archivo del procedimiento, que, a su juicio, se refieren hechos similares por los que a la recurrente se ha impuesto una sanción. En su opinión, la información de los expedientes que se indica y que tiene en cuenta la AEPD para denegar la falta de criterio es incompleta.

Alega asimismo que en todos los expedientes referenciados se consideró de forma positiva que las entidades víctimas de ciberataques tuvieran procedimientos de detección y gestión de brechas, circunstancia que no ha sido valorada como atenuante en el procedimiento que les afecta. También señala que las medidas por cuya ausencia se le ha sancionado en la resolución recurrida no fueran tampoco aplicadas por las entidades cuyos procedimientos se archivaron. Señala como ejemplos medidas como la psudonimización o el cifrado de la base de datos.

Entiende, en definitiva, que se le ha dado un trato discordante y discriminatorio.

CUARTA. - SOBRE EL SUPUESTO INCUMPLIMIENTO DEL ART. 32 RGPD

De nuevo se remite la recurrente a lo ya alegado durante la tramitación del procedimiento sancionador.

Considera que las cuestiones que han sido tenidas en cuenta para la constatación de la infracción son *insuficiencias menores, recomendaciones o deficiencias cuya relevancia para la seguridad general de los datos personales no ha sido probada, más allá de su puesta en relación con el resultado final de la brecha que se produjo como resultado de un ataque de excepcional e inusitada sofisticación.*

Destaca que el Informe emitido por SIA y aportado por la recurrente durante el procedimiento no pretendía valorar el nivel de seguridad de los sistemas, sino identificar qué ocurrió y cómo se produjo el ataque. Y recuerda el documento aportado con las alegaciones a la propuesta de resolución denominado “Anexo aclaratorio al Informe de análisis del incidente de ransomware”, que evalúa las medidas de seguridad implantadas de forma previa al incidente, y concluye que: “*las medidas de protección por parte de PHONE HOUSE eran adecuadas, pertinentes y proporcionadas, según el estado de la técnica” y que bajo ningún concepto, ninguna*

de las medidas que hubieran sido adoptadas, podrían haber evitado el brutal ataque que sufrió PHONE HOUSE.

Esta conclusión entiende que no ha sido desvirtuada por ningún mejor criterio y le permite señalar que la AEPD ha realizado una interpretación libre de lo contenido en dicho informe que le ha permitido alcanzar conclusiones opuestas.

Rechaza la recurrente el argumento que recoge la resolución recurrida para rebatir las conclusiones alcanzadas por dicho informe aclaratorio: que no se reflejan hechos sino valoraciones sobre hechos o circunstancias y que su valor como prueba es el que correspondería a un informe de parte.

A juicio de la recurrente, estos argumentos no son válidos porque el informe SIA inicial, que la AEPD sí tuvo en consideración, no sólo contenía hechos objetivos, toda vez que *un informe técnico que constituyera una mera narración de hechos sin un posterior juicio de valor técnico carecería de sentido.* De hecho, considera que estas suposiciones y juicios de valor son utilizados por la propia AEPD al argumentar las definiciones de las medidas de seguridad que se achacan a la recurrente. Entiende, además, que ambos informes son solicitados por la recurrente y aportados por ésta al expediente; ambos son informes de parte sin que ello afecte a su validez, máxime cuando ambos están perfectamente fundamentados y cuando no existen otros informes de contraste que hubieran sido aportados por la AEPD.

Asimismo, y de forma contraria a lo que entiende la AEPD, el nuevo informe, Anexo SIA, sí rebate expresamente las conclusiones de la AEPD, de acuerdo con el criterio técnico de su autor, *experto informático que ha tenido oportunidad de analizar las evidencias y el entorno digital en que se obtuvieron, y cuya trayectoria profesional le permite opinar de forma cualificada sobre la adecuación de las medidas de seguridad adoptadas.*

Destaca la recurrente que la existencia de puntos de mejora o debilidades en la seguridad de un sistema no puede equipararse a una inadecuación de medidas, pues todo es susceptible de mejor siempre; por el contrario, las debilidades o deficiencias han de ponerse en contexto al objeto de determinar si provocan que el sistema sea inseguro. E, incluso aunque lo sea, no cabría deducir que se produce necesariamente una falta de diligencia.

Señala asimismo que la conclusión de la inadecuación de las medidas tiene como único sustento el resultado del ciberataque, sin ningún criterio técnico que lo sustente tal afirmación, más allá de deficiencias puntuales cuya relevancia para la seguridad no han sido contrastadas. Asimismo, señala que no se establece un nexo causal entre la inexistencia de las medidas y el éxito del ataque.

A continuación, la recurrente expone los puntos de análisis a los que corresponden las supuestas deficiencias detectadas:

- Sobre las Evaluaciones de impacto de privacidad.

A juicio de la recurrente, constan claramente delimitados los tratamientos de riesgo alto sobre los que se llevó a cabo una evaluación de impacto, por lo que no cabe extender las medidas recomendadas en dichas las evaluaciones de impacto a otros

tratamientos con los que, aunque puedan guardar relación, están claramente diferenciados en el registro de actividades.

Entiende que, aunque el tratamiento general de datos de clientes es masivo, eso no hace que le sean de aplicación las medidas propuestas específicamente para otros tratamientos, por más que coincidan en esta característica. De ello, concluye que no puede hablarse de que se determinase la implantación de medidas de anonimización/pseudonimización o cifrado para la base de datos general de clientes ni hablar en genérico de medidas recomendadas en las evaluaciones de impacto, ya que cada una contiene sus recomendaciones específicas, que no son intercambiables entre ellas, ni hacia otros tratamientos.

Considera que se confunde la realidad de los hechos y se imputa incumplimientos que no se corresponden con la realidad de lo acreditado en la instrucción al ampliar una recomendación efectuada para otro tratamiento distinto a la base de datos general de clientes, con el único objetivo de achacar a continuación el hecho de que no se cumpliese con las medidas propuestas.

Vuelve a hacer mención el recurso a los precedentes concluidos con archivo en los que también se producía un tratamiento masivo de datos y que no estaban cifrados.

- Sobre las contraseñas

Vuelve a señalar la recurrente la validez de las aclaraciones realizadas en el Anexo Aclaratorio SIA, con el que considera que *el experto informático completa su informe concluyendo sobre la adecuación de las medidas implantadas, cuestión sobre la que inicialmente no se le había pedido pronunciarse*

Considera que el análisis de la AEPD sobre el inventario de sistemas aportado por la recurrente no es correcto, ya que las supuestas deficiencias detectadas no consideran los códigos de identificación de los diferentes niveles de seguridad exigibles, según el nivel de riesgo de los sistemas derivado de los tratamientos de datos realizados en su seno. En este sentido, todos los sistemas están calificados como seguros o altamente seguros.

Además, entiende que el hecho de que algunos sistemas no tengan medidas no significa que no existan, especialmente en las contraseñas. En este sentido, cuando existe un sistema de validación principal por medio del directorio activo, como es el caso, éste es el que controla las condiciones mínimas de las contraseñas, con independencia de que la concreta aplicación a la que se dé acceso por medio del directorio activo no las contemple.

Se refiere también la recurrente al informe de evaluación de medidas técnicas elaborado por ***XXXXX*** y que sí se refiere específicamente a los sistemas en los que se tratan datos personales, se analiza el sistema de control de acceso a los sistemas de concluyéndose con el cumplimiento de las obligaciones que le incumben.

Considera que en el caso del texto extractado del informe referente a los plazos de revisión de usuarios se refiere a una cuestión relacionada con el procedimiento interno aprobado que no se cumple residualmente en algunas aplicaciones, sin que ello suponga que se genere un riesgo reseñable. Y que

En lo referente al uso del algoritmo MD5 el informe se refiere a que no es "plenamente seguro", cualidad que no puede proclamarse de casi ningún mecanismo de cifrado, si bien ello no supone que sea vulnerable de forma corriente, teniendo en cuenta que se trata de un algoritmo de 128 bits. De hecho, la propia Guía CCN-STIC-807 a la que la AEPD se remite, refiere que se han hallado "algunas debilidades".

Finalmente, considera que el hecho de que la política de contraseñas se haya actualizado no puede interpretarse como justificativo de ninguna deficiencia previa. El procedimiento se refiere a medidas mínimas, lo que no implica que no se puedan adoptar unas superiores ni que no estuviesen implementadas con anterioridad a su inclusión en la política.

- Sobre la seguridad perimetral

Además de las consideraciones previas sobre la no atención a las conclusiones recogidas en el Informe aclaratorio aportado por la recurrente y de la incorrección de considerar que el hecho de adoptar medidas tras el ataque refuerza la consideración de las medidas como inadecuadas, la recurrente insiste en que muchas de las medidas implantadas tras el ataque *están muy por encima de las recomendadas para un escenario de riesgos similares y suponen ir mucho más allá de la diligencia exigible.*

En este punto, también señala que debe tenerse en cuenta que los atacantes consiguieron hacerse con credenciales de un administrador del sistema, con lo cual, los hallazgos que identifica el Informe SIA corresponden con un entorno manipulado y que muchas de las deficiencias encontradas en la seguridad perimetral pueden derivarse de alteraciones realizadas por el usuario intruso, con capacidad para modificar la configuración del sistema realizada previamente por la recurrente.

- Sobre las acciones formativas

Además de las alegaciones ya realizadas durante la tramitación del expediente, la recurrente cuestiona la consideración de que los cursos de formación y concienciación que impartía a sus trabajadores incurriese en una vulneración de la normativa de protección de datos y critica su falta de fundamentación. Por el contrario, entiende que cuenta con un *plan robusto, exhaustivo y continuado de formación continua en materia de protección de datos y seguridad de la información* y que sus trabajadores *recibieron formación y concienciación sobre protección de datos.*

- Otras medidas

La recurrente alega que no puede cuestionarse la validez del informe anual del DPO debido a su fecha de emisión por cuanto, por su naturaleza, ha de realizarse al concluir el año analizado. Con relación a la falta de evidencias contenidas en el mismo, recuerda que no se trata de un informe de auditoría sino un reporte de actividades anuales, en línea con lo indicado por la AEPD respecto del contenido del informe anual del DPO.

QUINTA. - SOBRE LA EXISTENCIA DE UN CONCURSO DE INFRACCIONES

Insiste la recurrente en lo ya alegado a lo largo del procedimiento sancionador al entender que se dan las circunstancias para considerar que tiene lugar un concurso medial entre las supuestas infracciones del artículo 5.1.f) RGPD y el artículo 32 RGPD, por ser necesaria la ausencia de medidas técnicas y organizativas apropiadas para que una brecha de confidencialidad sea sancionable. Entiende que no es posible entender incumplido el art. 5.1 f) cuando la entidad contaba con medidas técnicas organizativas apropiadas, por lo que un incumplimiento de este precepto siempre requiere que se dé un incumplimiento del artículo 32 del RGPD.

Reitera que no comparte la valoración de la AEPD en el sentido de que las medidas referidas en el artículo 32 RGPD son solo medidas de seguridad, mientras que las del artículo 5.1.f) RGPD cubriría también otro tipo de medidas e insiste en no haber recibido respuesta motivada que justifique este argumento.

A juicio de la recurrente, la referencia al art. 83.3 RGPD en el caso de concurrencia de infracciones no es conforme con lo que establecen las Directrices 04/2022, que entiende que "*en caso de concurso de infracciones, la cuantía de la multa debe calcularse únicamente sobre la base de la infracción seleccionada con arreglo a las normas anteriores (infracción prevalente).*"; siendo el supuesto de unidad de acción el que quedaría regulado en el art. 83.3 RGPD.

Argumenta la recurrente que debe concluirse que se da un concurso de infracciones, y en consecuencia la cuantía de la multa debe calcularse únicamente con base en la infracción prevalente.

SEXTA. - SOBRE LA INADMISIBILIDAD DE LA RESPONSABILIDAD OBJETIVA

Alega la recurrente que la resolución recurrida se basa en la concurrencia del resultado – la brecha acometida por los atacantes – para considerar acreditada una falta de diligencia por su parte. Considera que se impone una responsabilidad objetiva, en la que, independientemente de las medidas desplegadas, se alude a la posibilidad de implementar medidas más restrictivas. Insiste en que el no haber implementado cierta medida –especialmente unas tan restrictivas -, que no viene exigida por ninguna norma, estándar, o criterio vinculante, no puede determinar la imposición de consecuencias sancionadoras.

Reitera que los datos objeto de tratamientos de alto riesgo, para los que se recomienda adoptar medidas adicionales, no son los afectados por la brecha; de ahí que no quepa argumentar una falta de diligencia al respecto.

Considera que no se ha acreditado una conducta culpable en la implementación de medidas previas a la brecha, ni actuación culpable que permita impedir el resultado, por lo que existe una falta de nexo causal.

Rechaza además que la entrada en vigor del RGPD suponga una extensión de la responsabilidad o modificaciones en los requisitos para sancionar la conducta de la persona jurídica. Una interpretación extensiva rechazada por el Tribunal de Justicia de la Unión Europea Sentencias relativas a los asuntos C-683/21 y C807/21.

SÉPTIMA. - DE LA NECESIDAD DE ACREDITAR UNA INFRACCIÓN CULPABLE PARA LA IMPOSICIÓN DE MULTA

Basándose en la jurisprudencia del TJUE que menciona en el apartado anterior, entiende la parte recurrente que las condiciones que deben concurrir necesariamente para la imposición de una sanción administrativa han de materializarse en una actuación u omisión culpable o deliberada del responsable del tratamiento.

Considera no se puede atribuir a la recurrente dicha actuación culpable, intencionada o negligente que, al contrario, ha de considerarse víctima de un ciberataque.

OCTAVA. – DE LAS 211 RECLAMACIONES RELACIONADAS CON LA BRECHA DE SEGURIDAD

La recurrente relaciona la caducidad de las actuaciones de investigación iniciadas el 20 de abril de 2021 con las 211 reclamaciones que fueron presentadas por afectados por la brecha y de las que no se le ha aportado información.

Cuestiona que la necesidad de seguir investigando no se entiende por cuando la solicitud de más evidencias no se realiza sino hasta transcurridos tres meses desde la notificación de la apertura de nuevas actuaciones.

Considera que la duración de las actuaciones supone una garantía del procedimiento sancionador y que su extensión debe justificarse adecuadamente. A su juicio, al afirmar la AEPD que estas 211 reclamaciones no han sido tramitadas individualmente entiende que la notificación que ha de realizarse a los mismos es su inadmisión a trámite, no la resolución del procedimiento sancionador que afecta a la recurrente. El hecho de que no se haya actuado así demuestra que esas reclamaciones sí han sido tenidas en cuenta en el procedimiento sancionador que le ha afectado y que, por lo tanto, deberían haberle sido aportadas.

NOVENA. - SOBRE LA PRUEBA

Considera que la valoración de la prueba ha sido parcial y diferenciada y reitera que no ha sido tenido en cuenta las afirmaciones del Informe aclaratorio SIA, circunstancia que le ha generado indefensión

DÉCIMA. - SOBRE LA AUSENCIA DE PROPORCIONALIDAD EN LA FIJACIÓN DE LA CUANTÍA DE LA SANCIÓN PROPUESTA

Subsidiariamente, la recurrente plantea la falta de proporcionalidad de la sanción impuesta. Cuestiona que no conste mención expresa a los elementos fácticos específicos en los que la AEPD identifica una falta de diligencia por la parte recurrente, más allá, de la mención genérica a la posibilidad de implementar medidas adicionales a las ya establecidas e implementadas en el momento del suceso del ataque. Alega por otro lado que la sanción impuesta no constituye elemento disuasorio ni confidencial.

(…).

Cuestiona la recurrente que, para la imposición de la multa, se haya tenido en cuenta el número de posibles afectados, pero sin que la cifra de 13 millones de afectados- que se corresponde con los usuarios y clientes de la recurrente- sea la cifra de interesados cuyos datos se hayan visto afectados.

DÉCIMA. - AGRAVANTES ASOCIADOS POR LA AEPD A LAS INFRACCIONES

Reitera la recurrente sus alegaciones en lo que respecta a la aplicabilidad de los factores agravantes realizadas en la resolución sancionadora.

1) Naturaleza y gravedad de la infracción (artículo 83.2 a) RGPD). Pero se hace referencia a millones" o "*número aproximado de afectados*", sin concretar siquiera el número de afectados.
2) Nivel de los daños y perjuicios sufridos. Considera que no se aporta prueba que acredite la publicación de los datos afectados por la brecha en la Deep web. Se trata, por lo tanto, de una agravante basada en elementos fácticos no acreditados.
3) Duración de la infracción. Reitera que los sistemas utilizados en las actividades de tratamiento de alto riesgo en las que se realizó una evaluación de impacto no se vieron afectados por la brecha. Entiende que para apreciar la agravante de la duración sería necesario identificar concretamente las medidas cuya ausencia prolongada y mantenida en el tiempo determinan tanto la comisión de la infracción como un aumento de su gravedad.
4) Intencionalidad o negligencia en la infracción. Considera que la culpabilidad exigida para aplicar esta agravante no se da al ser la recurrente víctima del y perjudicada por el ataque.
5) Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal. Destaca que las Directrices 04/2022 sobre el cálculo de multas administrativas, excluye la actividad y sector empresarial concreto del infractor como criterio a considerar en la imposición y cuantificación de sanciones derivadas de una infracción de la normativa en materia de protección de datos. Entiende que el artículo 83.2 k) del RGPD exige que dicho agravante se ponga en relación con el supuesto concreto y, puesto que el tratamiento de datos tiene lugar la comisión de un delito del que la parte recurrente es parte perjudicada, no cabe interpretar este aspecto como agravante.

UNDÉCIMA. - SOBRE LA CONCURRENCIA DE FACTORES ATENUANTES NO CONSIDERADOS

Reitera las alegaciones previas sobre la aplicación de atenuantes a la conducta sancionada, especialmente al hecho de que se actuase de forma diligente en la gestión de la brecha y se adoptasen las medidas necesarias para mitigar los efectos de la brecha y reforzar la seguridad de sus sistemas. Una atenuante que ya se consideró en un caso precedente de naturaleza similar.

DUODÉCIMA. - SOBRE LA ADOPCIÓN DE MEDIDAS

Sobre las medidas impuestas en la resolución recurrida, insiste la recurrente en que los tratamientos de datos que realizaba ya se encontraban adecuados a la normativa de protección de datos en el momento en el que aconteció el ciberataque. También incluye como anexo las medidas adicionales que han sido adoptadas.

Adjunta asimismo la recurrente el listado de empleados que realizaron formación en protección de datos en 2023, junto con un vídeo explicativo del origen del listado, así como la cifra actualizada de trabajadores de la Compañía.

FUNDAMENTOS DE DERECHO

I
Competencia

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP) y el artículo 48.1 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).

II
Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, cabe en primer lugar destacar que las mismas suponen básicamente una reiteración de las alegaciones ya presentadas a lo largo del procedimiento sancionador, como la propia recurrente afirma al exponerlas de nuevo en el recurso. Correlativamente, por lo tanto, ha de señalarse que todas ellas ya fueron analizadas y desestimadas en la Resolución recurrida, en los siguientes términos:

En lo relativo a la primera de las alegaciones, eso es a la falta de motivación de la propuesta de resolución, ha de señalarse la misma fue atendida en las páginas 160 a 162 de la resolución recurrida, a cuyos términos, y en aras de la economía procesal, nos remitimos. Interesa no obstante recordar que, según indicábamos:

> *Además, procede recordar la reciente Sentencia de 9 octubre de 2023 de la Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección1ª, Rec. 1710/2021, que indica lo siguiente:*
>
> > *"En cuanto a la nulidad de la Resolución por motivación deficiente y defectuosa, hay que señalar que la exigencia de motivación de los actos administrativos viene impuesta con carácter general por el art. 35 de la Ley 39/2015, de 1 de octubre; la motivación responde a una triple necesidad ya que, por una parte, expresa que la Administración, al realizar la interpretación de la voluntad de la norma, ha actuado de una forma razonable; en segundo lugar, los destinatarios del acto pueden conocer esas razones y, eventualmente, someterlas a crítica y, por*

último, permite la fiscalización por parte de los tribunales de lo contencioso en los recursos contra el acto o disposición impugnados, con el alcance previsto en el art. 106.1. CE, y satisfacer así adecuadamente el derecho a la tutela judicial proclamado en el art. 24.1. CE.

Desde esta triple perspectiva, la motivación de un acto o disposición ha de ser puesta en relación con la concreta pretensión deducida en el proceso y con los motivos de impugnación aducidos por la parte, pues únicamente se podrá anular el acto por esta causa cuando la falta de conocimiento por parte del recurrente de las razones por las que la Administración ha actuado en la forma en que lo ha hecho le han impedido articular los medios de defensa y plantear su pretensión en consecuencia, de modo que sólo cuando el desconocimiento de aquéllas razones han provocado materialmente indefensión, vetada por el art. 24.2. CE, procedería anular el acto impugnado.

Como ha recordado el Tribunal Supremo en la sentencia de 20 de septiembre de 2012: «[...]la exigencia de motivación de los actos administrativos constituye una constante de nuestro ordenamiento jurídico y así lo proclama el artículo 54 de la LRJPA (antes, artículo 43 de la Ley de Procedimiento Administrativo de 17 de julio de 1958), teniendo por finalidad la de que el interesado conozca los motivos que conducen a la resolución de la Administración, con el fin, en su caso, de poder rebatirlos en la forma procedimental regulada al efecto. Motivación que, a su vez, es consecuencia de los principios de seguridad jurídica y de interdicción de la arbitrariedad enunciados por el apartado 3 del artículo 9 de la Constitución Española (CE) y que también, desde otra perspectiva, puede considerarse como una exigencia constitucional impuesta no sólo por el artículo 24.2 CE, sino también por el artículo 103 (principio de legalidad en la actuación administrativa)". (el subrayado es nuestro)

Por tanto, la Propuesta de Resolución, al contener motivadamente (recordemos que la Ley sólo exige de modo sucinto) todos y cada uno de los extremos que exige la LPACAP, TPHS ha podido conocer los hechos que se consideran probados y su exacta calificación jurídica, la infracción que, en su caso, aquéllos constituyan y la sanción que se ha propuesto así como la valoración de las pruebas practicadas, ha permitido con ello que TPHS haya podido formular las alegaciones y aportado los documentos que ha estimado pertinentes para la defensa de sus derechos e intereses.

Ha de concluirse, por lo tanto, que la parte recurrente ha podido ejercer en todo momento a lo largo de la tramitación del procedimiento sancionador su derecho a la defensa, conociendo en todo momento los hechos que se le imputan y las infracciones derivadas de los mismos, sin que del rechazo por parte de esta AEPD de los argumentos reiteradamente esgrimidos, en base a razonamientos debidamente motivados, pueda extraerse una *falta de esfuerzo para entender lo expuesto* como alega la recurrente.

En lo que respecta a la coincidencia fáctica de las infracciones imputadas, toda vez que constituye el centro de la alegación referida a la existencia de un concurso de infracciones, nos remitimos a la respuesta a esta alegación que realizamos en apartados posteriores de la presente reclamación.

Por todo cuanto se indica, esta alegación ha de ser desestimada.

Reitera de nuevo la recurrente que el análisis de los hechos objeto del expediente sancionador ha de partir de su consideración como parte afectada y víctima del ciberataque del que trajo causa la brecha de datos personales por la que se le sanciona. Se trata de un argumento que la parte recurrente lleva esgrimiendo desde las alegaciones al acuerdo de inicio adoptado con fecha 27/03/2023 y que ha reiterado en todas las fases procedimentales. Un argumento que, por otro lado, ha sido justificadamente rechazado por esta AEPD en la resolución recurrida: en las páginas 69 a 71 al responder las alegaciones al acuerdo de inicio y en las páginas 162 a 167 al responder a las alegaciones a la propuesta de resolución. Si bien nos remitimos a lo señalado, conviene recordar algunos de los razonamientos realizados:

> *Frente a ello, procede remitirse a lo ya respondido sobre esta cuestión en la Propuesta de Resolución y que se reproduce en el Antecedente de Hecho Noveno, apartado Primero. Así, en la misma se indicó que en ningún caso se ha exigido una infalibilidad total de las medidas que se pueden adoptar para garantizar una protección adecuada en el tratamiento de los datos personales. Sin embargo, una vez producido el ataque, debe evaluarse la diligencia del responsable del tratamiento en la aplicación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniéndose en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento.*
>
> *En el presente caso, ya se señaló que TPHS no contaba, en el momento de producirse la brecha de protección de datos, con las medidas adecuadas en relación con los riesgos del tratamiento para la protección de los datos personales, pues tal y como se indicó en el Acuerdo de Inicio del presente procedimiento sancionador, y que se reseña nuevo en el Fundamento de Derecho VII de esta Resolución y al que procede remitirse, existían deficiencias en relación con:*
>
> > *1.- la política de contraseñas y demás restricciones para el acceso a los sistemas de información de TPHS.*
> > *2. la protección de la seguridad perimetral y de las medidas de monitorización para la detección de conducta maliciosa;*
> > *3. la formación y concienciación de los empleados.*
>
> *Asimismo, no tenía implantadas las medidas de seguridad que, respecto a los tratamientos afectados por la brecha, había indicado en sus propias EIPDs que debían implantarse, a la vista de los riesgos altos y muy altos arrojados (seudonimización, cifrado, anonimización…). Por tanto, las medidas de seguridad no eran adecuadas a los riesgos, tal y como exige el artículo 32 del RGPD, y ello con independencia del concreto ataque sufrido.*

Reitera de nuevo la recurrente las inversiones realizadas con carácter previo a la brecha y también con posterioridad a la misma. Sin perjuicio de que nos reafirmamos en el argumento de que *los gastos posteriores derivados del ataque no pueden entenderse como reflejo de una diligencia de TPHS antes de producirse la brecha, más al contrario, pues muchas de las medidas que ha implantado después debían de haber estado implantadas con anterioridad para haber garantizado una seguridad adecuada en función del riesgo,* ha de señalarse que, respecto de la inversión previa que recuerda la recurrente, las medidas técnicas y organizativas de seguridad han de ser no sólo adecuadas sino que las mismas han de implantarse y utilizarse con una diligencia razonable.

Asimismo, consideramos que, con la mención al importe de inversión realizado no sólo no se justifica que las medidas fueran las adecuadas, sino tampoco que fueran debidamente implementadas y, sobre todo, que fueran eficaces para hacer frente a los riesgos derivados del tratamiento de datos realizados. Máxime cuando con posterioridad a la implantación de dichas medidas- con una elevada inversión a juicio de la recurrente- se produjo la brecha de datos personales por la que se sanciona.

Por lo tanto, esta alegación ha de desestimarse.

En relación con el *supuesto incumplimiento del artículo 5.1 f) RGPD,* comencemos indicando la respuesta proporcionada al respecto en las páginas 71-72 (respuesta a las alegaciones al acuerdo de inicio) y 167-171 (respuesta a las alegaciones a la propuesta de resolución) contenida en la resolución recurrida.

Considera ahora la recurrente que es incompleto el reflejo en la resolución dictada de los precedentes por ella señalados y que, a su juicio, demuestran una diferencia de criterio respecto al que se le ha aplicado (puesto que previamente, en situaciones similares en su opinión, la AEPD ha resuelto con el archivo del procedimiento); circunstancia que no permite hacer una valoración adecuada de los hechos presentes en dichos procedimientos y que permita la comparativa con el presente.

En respuesta a esta alegación ha de recordarse lo ya señalado en la resolución sancionadora, en los siguientes términos:

> *Frente a ello, ya se le indicó entonces que esta Agencia no tiene un criterio de archivo en el supuesto de ciberataques, del tipo que sea, ni tampoco, por tanto, respecto de aquellos afectados por un ransomware, sino que, en materia de protección de datos, las medidas técnicas y organizativas de seguridad a adoptar por los responsables del tratamiento y demás obligaciones a cumplir exigidas por el RGPD, deben ser las adecuadas en relación con los concretos riesgos que suponen los específicos tratamientos que realice cada responsable. Por tanto, al analizar la diligencia de unos y otros en el cumplimiento de la normativa ha de estarse a las circunstancias de cada caso, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines de cada tratamiento, no existiendo, por tanto, casos idénticos. Así, un ataque realizado con el mismo ransomware en el mismo momento y en distintas empresas tendría resultados dispares, pues las circunstancias son diferentes. Incluso*

> *este mismo ataque contra la misma empresa en momentos distintos podría determinar una situación diferente.*

Por lo tanto, por mucho que se empeñe la recurrente en señalar precedentes, de los años 2019, 2020 y 2021, cuyos hechos, a su juicio, son similares, difiriendo la respuesta de la AEPD, ese pretendido ejercicio de comparación no cabe aplicarse por cuanto, como ya señalábamos, no existen casos idénticos, sino que, antes al contrario, habrá de estarse a las determinadas circunstancias presentes en cada uno de ellos.

A lo anterior, cabe señalar que la pretendida coincidencia en cuanto a los hechos objeto de análisis en los precedentes que mencionan parte de una visión, esta sí, incompleta de las circunstancias acaecidas en los mismos por cuanto, como ya decíamos en la resolución recurrida *Por otro lado, en la mayoría de las Resoluciones se omite en su publicación en la web de la Agencia todo lo relacionado con concretas medidas de seguridad que resultan confidenciales en aras de proteger la seguridad de las entidades, por lo que no es posible poner de manifiesto las circunstancias tenidas en cuenta relacionadas con medidas concretas de seguridad de la información*.

Es decir, es la AEPD la que dispone de todos los elementos de juicio para valorar las circunstancias presentes en los procedimientos que insiste en señalar la recurrente y concluir que las mismas difieren de las presentes en el procedimiento sancionador del que ha sido parte. No ha existido, por lo tanto, una diferencia de trato que haya perjudicado a la recurrente sino una respuesta de esta Autoridad de Control que atiende a las especiales características y circunstancias de cada uno de los procedimientos analizados.

En definitiva, como ya indicábamos:

> *En varios de estos casos no consta que se produjera una vulneración de la confidencialidad, limitándose el incidente al cifrado transitorio o bien recuperaron el 100% de los datos debido a backups; existían medidas técnicas y organizativas apropiadas; habían sido objeto con anterioridad reciente de auditorías (muchas de ellas de certificaciones de conformidad con norma ISO 27001 sin obtener ninguna no conformidad; el número de afectados es diferente, etc. En fin, que no hay dos casos iguales incluso frente a un ataque similar por cuanto las empresas son diferentes, se encuentran en el momento del ataque con medidas de seguridad propias y diferentes cada una, los efectos para los interesados son diferente, etc.*
>
> *De todo lo expuesto se concluye que no hay dos expedientes iguales, que, en ellos, las actuaciones previas de investigación llevadas a cabo por la AEPD pusieron de manifiesto que no existían evidencias de infracción para el caso concreto, que tenían medidas adecuadas, que no se exfiltró información o que no se accedió por terceros, que se afectó sólo la disponibilidad pero que se pudieron recuperar los datos gracias a la existencia de copias de seguridad, etc…*
>
> *Por tanto, no son susceptibles de comparación con las circunstancias del presente caso, pues se trata de organizaciones muy diferentes bien por su tamaño (muchas de ellas PYMES), por los tratamientos que realizan, la*

tipología de los mismos, los datos personales involucrados, los riesgos existentes, los sistemas afectados, por el momento tecnológico en el que opera en cada ciber incidente; de hecho, ni siquiera el malware usado es el mismo ni ha utilizado los mismos métodos de ataque, número de personas afectadas, medidas implementadas antes del incidente, etc.

Por último, no se puede comparar ninguno de ellos con el número de afectados por la brecha de datos personales sufrida por TPHS, que afectó a 13 millones de personas.

Por lo expuesto, no existe en esta Agencia un criterio de archivo, ni de importes concretos de las sanciones a imponer en su caso, ni de las infracciones concretas a imputar en el caso de ciberataques, ya sean estos de tipo ransomware o de otro tipo, pues incluso en los supuestos de ransomware, como se ha señalado, se atiende especialmente al modus operandis del ataque y al resto de circunstancias concretas, en particular y especialmente, las medidas previas de seguridad existentes.

Para demostrar la falta de consistencia de las alegaciones recogidas en el recurso de reposición, basta señalar que la recurrente señala que *(…) habida cuenta de que en ninguno de los mencionados procedimientos esta Agencia entra siquiera a valorar el potencial incumplimiento del at. 5.1 f) RGPD.* Al respecto, cabe recordar que el incumplimiento del art. 5.1 f) no puede ser "potencial" sino que se refleja en una efectiva pérdida de confidencialidad de los datos, materializándose en que los mismos sean conocidos por terceros sin que exista justificación para ello. Asimismo, no puede valorarse un posible incumplimiento de dicho precepto si, tal y como señalábamos en la resolución en varios de dichos precedentes se constató *que no se exfiltró información o que no se accedió por terceros, que se afectó sólo la disponibilidad pero que se pudieron recuperar los datos gracias a la existencia de copias de seguridad etc…*

Por el contrario, y tal y como se razona en la resolución recurrida (página 75)

Por tanto, en el supuesto examinado, tal y como consta en los hechos probados, hay una clara pérdida de confidencialidad pues se ha producido el acceso por un tercero no autorizado a los datos personales tratados por TPHS, siendo ello un resultado objetivo, reconocido por TPHS, que no una responsabilidad objetiva. No se ha garantizado, de esta forma, una seguridad adecuada mediante la aplicación de las medidas técnicas y organizativas apropiadas, no sólo de seguridad, sino de todo tipo.

Respecto de la valoración positiva de procedimientos de detección y gestión de brechas que entiende la recurrente se realizó en los precedentes mencionados, además de reiterarnos de que el criterio de esta AEPD se conforma en atención a las circunstancias concurrentes en cada caso, no cabe sino recordar que la notificación de una brecha de datos personales es una obligación del responsable del tratamiento de datos recogida en el artículo 33 del RGPD y, en buena lógica, sólo podría cumplirse esa obligación con un adecuado procedimiento de detección y gestión de brecha. Recuérdese también que el incumplimiento de esta obligación supone una infracción de acuerdo con lo previsto en el artículo 83.4 a) del RGPD.

Por lo tanto, esta alegación ha de desestimarse.

Plantea a continuación la recurrente alegaciones con relación al *supuesto incumplimiento del art. 32 RGPD*, con argumentos ya extensamente analizados- y rebatidos- en las páginas 75 a 90 y 171 a 193 de la resolución recurrida.

Como puede observarse, en el recurso, la recurrente vuelve a cuestionar la valoración que realiza esta AEPD del contenido del "Anexo aclaratorio al Informe de análisis del incidente de ransomware" cuestión que ya fue planteada- y respondida- durante la tramitación del procedimiento.

Comencemos recordando que, tal y como ya se le indicó a la recurrente *En primer lugar, esta Agencia no se ha basado únicamente en lo declarado en el Informe SIA, sino que también ha tenido en cuenta toda la documentación aportada y recabada durante las actuaciones previas de investigación, en la cual se han puesto de manifiesto numerosas deficiencias o falta de medidas que han reflejado una clara infracción del artículo 32 RGPD (…).* Es decir, no es que esta Autoridad decidiera a su antojo la documentación a valorar y tener en cuenta, sino que se realizó un análisis de toda la documentación contenida en el expediente. De nuevo, la recurrente parece querer escenificar una especie de falta de rigor en el trabajo desempeñado por esta Agencia cuando, simplemente, lo que se ha producido es un rechazo- debidamente fundamentado en todo momento- de las alegaciones esgrimidas. No ha existido, aunque la recurrente insista en plantearlo, una "interpretación libre" por parte de la AEPD, sino una valoración rigurosa, de acuerdo a criterios técnicos y jurídicos, de los hechos acaecidos, las implicaciones para el derecho a la protección de datos personales, y la respuesta jurídica que, frente a este tipo de hechos, prevé nuestro ordenamiento.

Insiste la recurrente en considerar que las conclusiones del denominado *Informe Aclaratorio SIA* sí rebate las conclusiones alcanzadas por la AEPD y, para ello, alude al criterio técnico del *único experto informático que ha tenido la oportunidad de analizar las evidencias y el entorno digital en que se obtuvieron, y cuya trayectoria profesional le permite opinar de forma cualificada sobre la adecuación de las medidas de seguridad adoptadas, gozando de los "conocimientos científicos, artísticos, técnicos o prácticos" precisos para emitir dictamen*. Se olvida la recurrente de que es la AEPD la que no sólo ha tenido un conocimiento completo de las circunstancias acaecidas- no únicamente por la documentación aportada durante la tramitación, sino por la propia actuación de investigación desarrollada- sino la que aglutina el conocimiento técnico y jurídico, no sólo teórico sino práctico, para valorar conveniente dichas circunstancias y concluir- y fundamentar- qué consideración jurídica han de tener.

No podemos compartir el argumento esgrimido en el sentido de que *puntos de mejora o debilidades en la seguridad de un sistema no puede equipararse, como hace la AEPD, a una inadecuación de medidas*; antes al contrario, esas debilidades son las que, precisamente, se evitan con la adopción e implementación de medidas adecuadas en atención al riesgo derivado del tratamiento de datos realizado. La existencia de una debilidad- y más si es constatada- es una puerta abierta a una situación de vulneración de la seguridad de los datos.

Insiste de nuevo la recurrente en volver a mencionar los cuatro aspectos sobre los que se detectaron deficiencias: implementación de medidas relacionadas con las Evaluaciones de Impacto de Protección de Datos (EIPD), la política de contraseñas implementadas, la seguridad perimetral y la formación de usuarios. Cabe destacar que la recurrente no aporta argumento nuevo y que todas las cuestiones planteadas fueron ya atendidas en la resolución sancionadora en los siguientes términos:

- Implementación de medidas relacionadas con las EIPDs: páginas 178 a 185

Insiste la recurrente en cuestionar que se extiendan las medidas recomendadas en las EIPDs realizadas con relación a tratamientos de riesgo alto, a otros tratamientos distintos y que se encuentran diferenciados en el Registro de Actividades de Tratamiento; incluso aunque coincidan en la característica de tratarse de un tratamiento de datos masivo. Se trata, como los anteriores previamente analizados en la presente resolución, de un argumento reiteradamente planteado y contestado, igualmente de forma reiterada:

> *En segundo lugar, señala TPHS que los tratamientos de "marketing digital" y al "control de acceso a las instalaciones", nada tienen que ver con los datos afectados por la brecha sufrida. Insiste de nuevo que los tratamientos relativos a las EIPDs aportadas no han sido afectados por la brecha de seguridad, por lo que no puede existir causalidad alguna entre dichos tratamientos y la brecha de seguridad, que entiende que es el único y exclusivo motivo por el que se le ha iniciado procedimiento sancionador.*
>
> *Asimismo, indica TPHS que la Agencia dispone del registro de actividades y de las PIAs porque se las requirió sin matizar que deseaba recibir el registro de actividades de los tratamientos afectados por la brecha de seguridad o las EIPDs de los tratamientos implicados en el ciberataque, por lo que, en aras de la máxima transparencia, se facilitó toda la información contenida en el registro de tratamientos.*
>
> *A este respecto, procede reiterarse a todo lo argumentado en relación con este tema en el apartado Segundo de este Fundamento de Derecho, al que nos remitimos, tanto en relación con el hecho de que con independencia de la brecha de datos personales sufrida, TPHS no tenía implantadas las medidas de seguridad que ella misma había indicado en sus EIPDs dos años antes del incidente, lo que de por sí indica que no se habían aplicado las medidas apropiadas para garantizar una seguridad adecuada al riesgo, que en su caso incluya, entre otros: a) la seudonimización y el cifrado de datos personales, lo que supone un incumplimiento del art. 32 RGPD, como en el hecho de que sí se requirieron específicamente los análisis de riesgos y, en su caso, las EIPDs respecto de los tratamientos afectados por la brecha y fue TPHS la que indicó, en respuesta a los requerimientos de información efectuados durante las actuaciones previas de investigación, que entre los tratamientos afectados por la brecha de datos personales, se incluyen el "marketing digital" y el "control de acceso a las instalaciones". Por tanto, esas actividades de tratamiento sobre las que se realizaron las EIPDs aportadas por TPHS sí estaban afectadas por la brecha, tal y como indicó en las respuestas a los requerimientos realizados, en lo cual ahora simplemente se desdice.*

Con estas alegaciones, de nuevo ahora en fase de recurso, la recurrente no hace sino reafirmar la conclusión que alcanzamos: que la recurrente se desdice de lo manifestado durante la tramitación del procedimiento sancionador con la única intención de plantear dudas sobre la apreciación de esta Agencia en relación a la infracción competida.

Señala de nuevo la recurrente su disconformidad sobre el cuestionamiento del enfoque de las EIPDs que se realizó durante la tramitación del expediente, a pesar de que, como ella misma reconoce, esta cuestión no es objeto de la sanción impuesta. No podemos sino reiterarnos en la respuesta dada en la página 181 de la resolución donde, tras señalar

> *A este respecto, y con carácter previo y fundamental, se significa que en el presente procedimiento sancionador no se ha imputado a TPHS una infracción del artículo 35 RGPD por no cumplir las EIPD los requisitos exigidos por el RGPD, si no únicamente se le ha puesto de manifiesto que el enfoque no es correcto. Por tanto, no es una cuestión esencial en este procedimiento sancionador ni desvirtúa ello los hechos probados en los que se basan las infracciones imputadas.*
>
> *Asimismo, en cuanto que no se ha justificado esta interpretación, procede remitirse a lo argumentado en la Propuesta de Resolución en relación con esta misma alegación, que aparece transcrito en el Antecedente de Hecho Noveno, alegación Sexta, donde se ha explicado claramente las razones por las que se le ha indicado que el enfoque no es correcto en la mayoría de los riesgos indicados en las EIPDs aportadas.*

Se recoge a continuación, en las cuatro páginas siguientes, una profusa explicación de por qué se considera que el enfoque aplicado en las EIPDs no es el correcto.

- Política de contraseñas: páginas 185 a 188

Vuelve la recurrente a intentar hacer valer las conclusiones alcanzadas en el Informe Aclaratorio SIA pretendiéndole otorgar, de nuevo, un valor prevalente respecto incluso de los hechos reflejados en el informe que pretende aclarar. Al respecto, ya se señaló que

> *En este sentido, no se ha negado ni desvirtuado estos hechos o hallazgos, sino que se ha realizado una valoración de los mismos, frente a la que esta Agencia no está de acuerdo, por cuanto las mismas reflejan deficiencias importantes en cuanto a la política de contraseñas.*

Para, a continuación, señalar que

> *Asimismo, el Anexo SIA únicamente interpreta o valora ahora los hallazgos en el análisis del incidente y que plasmó en el Informe SIA. Sin embargo, tal y como se ha señalado anteriormente, a la hora de determinar la existencia de deficiencias en la política de contraseñas en el presente procedimiento sancionador no sólo se ha tenido en cuenta el contenido del Informe SIA sino*

también los informes de evaluación aportados por la empresa Écija (Informe "Evaluación del cumplimiento en materia de protección de datos – Medidas de Seguridad –",fechado el 11 de enero de 2021; Informe "Evaluación del cumplimiento en materia de protección de datos – Medidas de Seguridad –", fechado el 11 de enero de 2021; así como el inventario de sistemas aportado por TPHS el 28 de junio de 2021 (Número de registro: O00007128e2100028705). Por último, también se ha tenido en cuenta las medidas que TPHS declaró haber implantado o en proceso de implantación con posterioridad a la brecha.

En dicha documentación se reflejó -tal y como se ha señalado pormenorizadamente al principio de este apartado Cuarto de respuesta a las alegaciones, al cual procede remitirse- numerosas e importantes deficiencias las cuales no han sido desvirtuadas y que reflejan medidas inadecuadas por parte de TPHS y que no aparecen en el Informe SIA.

Todo ello pone de manifiesto que, con independencia de la brecha de datos personales detectada, la política de contraseñas y demás restricciones para el acceso a los sistemas de información de TPHS no eran adecuadas para garantizar una seguridad apropiada, suponiendo vulnerabilidades aprovechables por cualquier atacante. No debe olvidarse, como se ha señalado, que en el informe de SIA se apunta que se ***(…).***

De ello se deduce que es una valoración lo indicado ahora en el Anexo SIA relativo a que "lo más habitual en estos casos es que un ataque de ingeniería social permitiese obtener dichas credenciales engañando a un usuario con permisos de administración", es decir, podría haber sido un ataque de phishing, pero también haber sido igualmente por los otros tres posibles vectores de entrada que se indicaron en el Informe SIA, los cuales apuntan todos a deficiencias en la política de contraseñas.

En relación a lo alegado respecto del uso del algoritmo MD5, al que el informe se refiere como que no es "plenamente seguro", señala que *ésta es una cualidad que no puede proclamarse de casi ningún mecanismo de cifrado, si bien ello no supone que sea vulnerable de forma corriente (…)*

Frente a ello, no cabe sino remitirnos a lo indicado en la resolución recurrida:

A este respecto, procede señalar que la deficiencia del algoritmo de encriptado es una verdadera deficiencia, un algoritmo nada seguro y ya puesto ello de manifiesto años antes por el CCN, aunque fuera recogido como recomendación en el informe señalado. Lo que refleja el informe es que TPHS estaba utilizando ese algoritmo y que el mismo es deficiente lo cual se conoce desde hace años. No debe olvidarse que el atacante consiguió las credenciales de varios usuarios de TPHS.

En definitiva, la recurrente conocía desde hace tiempo que el algoritmo que estaba utilizando era deficiente y, a pesar de ello, no fue lo suficientemente diligente como para usar otro. Teniendo en cuenta que el ataque que supuso la brecha de datos personales fue motivado por el acceso a las credenciales de varios usuarios de la

parte recurrente, esta falta de diligencia tuvo una consecuencia directa y objetiva, en las causas de la brecha y, por lo tanto, en sus consecuencias.

Finalmente, cabe recordar, en lo que respecta a la política de contraseñas que en la resolución sancionadora se señala expresamente que

> *Procede recordar, además, que no existía tampoco otra medida conocida y asequible según los costes y el estado de la técnica actual, como es el doble factor de autenticación que no tenía implantado en el momento del incidente, ni tan siquiera para usuarios con perfil de administrador, pues según manifestó expresamente TPHS lo tenía "en proceso de implantación".*

- Seguridad Perimetral 188 a 192

Insiste la recurrente en la calidad de las medidas adoptadas y que las implementadas tras el ciberataque están *muy por encima de las recomendadas para un escenario de riesgos similares y suponen ir más allá de la diligencia exigible.* Al respecto, sólo cabe aducir algo que es obvio pero que parece que la recurrente no lo considera así: el expediente sancionador iniciado y frente a cuya resolución se interpone recurso de reposición tiene en cuenta las medidas vigentes en el momento del ataque, que facilitaron el mismo y, en consecuencia, la brecha de datos personales por la que se sanciona.

En este sentido, y frente a las medidas que la recurrente alegó que adoptó o que indica "en proceso de implantación" tras el incidente y que, por tanto, no tenía implantadas, se contestó lo siguiente:

> *Sin embargo, TPHS no las tenía implementadas. Ello le hubiera permitido la posibilidad de haber detectado la conducta maliciosa del atacante durante 11 días (entradas y salidas por el ciberdelincuente desde IPs situadas en países como Bulgaria y Moldavia o desde nodos TOR, sus movimientos por la red, fuga de información, etc). Desde luego, sin ellas, no hubo opción de ello.*

Cuestiona de nuevo las conclusiones alcanzadas en el informe especializado (Informe SIA) aportado por la recurrente intentando descalificar sus hallazgos señalando que los mismos se corresponden con *un entorno manipulado y que muchas de las deficiencias encontradas en la seguridad perimetral pueden derivarse de alteraciones realizadas por el usuario intruso (…).* La recurrente parece olvidar que, precisamente, el intruso tuvo capacidad para introducirse en sus sistemas por las deficientes medidas de seguridad implantadas, y ello sin perjuicio de que no aporta ninguna prueba o evidencia que permita alcanzar la conclusión que manifiesta.

- Sobre la formación de usuarios: 192

La recurrente califica como patente error en la valoración de la prueba que ha efectuado la AEPD lo que, simplemente, es una valoración que no comparte y de la que se desprende un palmario incumplimiento de la normativa de aplicación. Pretender atribuir a una falta de rigor el hecho de que las alegaciones planteadas no hayan sido acogidas no es aceptable.

De nuevo realiza consideraciones sobre las medidas adoptadas en relación a la formación de sus empleados que, utilizando en el recurso los exactos mismos términos que en sus alegaciones a la propuesta de resolución, califica de *plan robusto, exhaustivo y continuado de formación continua en materia de protección de datos y seguridad de la información.*
Sobre este punto, no cabe sino remitirnos, de nuevo, a lo señalado en la resolución recurrida:

> *Respecto a lo alegado por TPHS en relación con la formación, ya que ello es reiteración de lo manifestado frente al Acuerdo de Inicio, procede remitirse a la respuesta dada en la Propuesta de Resolución, la cual aparece transcrita en el Antecedente de Hecho Noveno, alegación Novena. Asimismo, procede remitirse a lo indicado en la respuesta a la alegación Primera de este Fundamento de Derecho. Allí, se respondió analizando la documentación aportada por TPHS relativa a la formación. Así, se indicó que "analizada la documentación cabe reseñar que la mayoría refleja cursos genéricos y no acredita cuántos alumnos ni cuándo se realizaron (documento 4); curso genérico sin que acredite quiénes lo realizaron y no resulta obligatorio (pantallazo de un mail enviado el 17 de noviembre de 2019); curso dirigido a TPHS, a sus obligaciones como responsable de tratamiento (documento 6); cursos genéricos on line a realizar por los trabajadores nuevos contratados a partir de 2018, acompañado de un listado de unos 330 personas que lo han realizado, sin fechar ni firmar".*

Realiza la recurrente otra serie de alegaciones bajo la rúbrica "Otras medidas" en las que se hace referencia a la puesta en duda por parte de la AEPD de la validez del informe anual del Delegado de Protección de Datos (DPO) debido a su fecha de emisión (se refiere al año 2021 pero fue adoptado al finalizar el mismo, en enero de 2022) y a que el mismo no aporta evidencias- *lo cual no sería posible al no tratarse de una auditoría*. Cabe señalar al respecto que fue la propia recurrente la que aportó el informe de su DPO en el procedimiento y, por lo tanto, la que le intentó dotar de una especie de naturaleza probatoria que, sin embargo, ahora parece restarle para justificar la ausencia de evidencias.

> Página 109*: Señala TPHS que había implementado, con carácter previo a la brecha de seguridad, todas las recomendaciones derivadas del "Informe de Evaluación Técnico", así como del "Informe de Evaluación Jurídico-Organizativo" emitidos por una entidad externa, tal y como ha quedado acreditado de las distintas pruebas aportadas por esta parte, así como del contenido del "Informe anual de Delegado de Protección de Datos de 2021", entregado a esta AEPD (vid. páginas 1544 y 1545 del Expediente Administrativo):*
>
> Página 137*: Adicionalmente, es interés de TPHS traer a colación en este punto el "Anexo aclaratorio al Informe de análisis del incidente de ransomware", así como el "Informe anual de Delegado de Protección de Datos de 2021" (vid. páginas 1542 a 1552 del Expediente Administrativo), a fin de acreditar que TPHS contaba con medidas técnicas y organizativas apropiadas para*

garantizar un nivel de seguridad adecuado al riesgo, en el momento en el que sufrió el ciberataque.

Por otro lado, no se cuestiona que un informe referido al año 2021 sea elaborado con posterioridad, en este caso, en enero de 2022, pero sí que, siendo *muy posterior al incidente, no teniendo por tanto el valor pretendido por TPHS como prueba para acreditar fehacientemente que en el primer trimestre del año estaban implementadas esas medidas, las cuales, además, no guardan relación con las señaladas.*

Por lo tanto, esta alegación ha de desestimarse.

Con relación a las alegaciones relacionadas con la existencia de un concurso de infracciones que alega la recurrente de nuevo nos encontramos ante la reiteración de argumentos ya expuestos y rebatidos debidamente.

Como ya se señalaba en la resolución recurrida (alegaciones al acuerdo de inicio, página 96-97)

Pues bien, el art. 5.1.f) del RGPD recoge el principio de integridad y confidencialidad y determina 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 y de todo tipo, no sólo de seguridad.

Por otra parte, el art. 32 del RGPD reglamenta cómo ha de articularse la seguridad del tratamiento en relación con las medidas de seguridad concretas que hay que implementar, de tal forma que teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluya entre otras cuestiones, la capacidad de garantizar la confidencialidad de los datos.

Como se ha señalado, este precepto, el art. 32 del RGPD, aunque relacionado con el art. 5.1.f) del RGDP no circunscribe el principio en su totalidad. El art. 5.1.f) del RGPD exige taxativamente que se garantice la confidencialidad, y requiere para su aplicación una pérdida de confidencialidad. Podemos encontrarnos con supuestos en que existan medidas inadecuadas sin que por ello haya una pérdida de integridad y confidencialidad. (…)Indica TPHS que las medidas técnicas y organizativas apropiadas a las que hace mención el artículo 5.1.f) son las medidas de seguridad del art. 32 del RGPD. Esto sería simplificar la esencia del RGPD cuyo cumplimiento no se limita a la implantación de medidas técnicas y organizativas de seguridad; significaría, en nuestro caso, reducir la garantía exigida mediante el principio de integridad y confidencialidad a su logro únicamente con medidas de seguridad. (…)

Por lo expuesto, en el presente caso, la ausencia de unas concretas medidas de seguridad que van dirigidas específicamente a garantizar la confidencialidad, a saber, el cifrado y la pseudonimización (o la anonimización) es lo que ha traído como consecuencia la existencia de la brecha de confidencialidad de los datos personales. Si los datos hubieran estado cifrados, anonimizados o pseudonimizados, los delincuentes sólo se hubieran llevado información ininteligible. De ahí que se le impute a TPHS la infracción del artículo 5.1.f), pues el mismo exige garantizar la confidencialidad a través de diversas medidas, que pueden ser tanto de seguridad como de otro tipo.

Sin embargo, la infracción del artículo 32 del RGPD que se le ha imputado, lo ha sido por la falta o la inadecuación de numerosas medidas, esta vez sí, dirigidas a garantizar un nivel de seguridad adecuado al riesgo de los tratamientos que se realizan. Y de todas las medidas de seguridad que se detectan que faltan o que eran inadecuadas y que suponen una vulneración del artículo 32 RGPD -las cuales se indican en el Fundamento de Derecho VII de la presente Propuesta, al que nos remitimos-, sólo hay dos, que han resultado determinantes para la pérdida de confidencialidad: de nuevo, el cifrado y la pseudonimización o la anonimización).

Por tanto, en el presente caso se ha infringido el citado artículo 32 con independencia de si se ha sufrido finalmente una brecha de confidencialidad o no, porque la conducta reprochable y que vulnera dicho precepto es la falta o inadecuación de esas medidas, en sí mismas, es decir, se infringe y se sanciona por ello con independencia de si se ha producido una brecha de datos personales o no. (…)

Frente a ello, se señala que, en relación con la cita de las Directrices 04/2022 del CEPD sobre el cálculo de multas administrativas conforme al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, en su apartado 22 se hace referencia a tres tipos de concurrencias, a saber, de infracción, unidad de acción y pluralidad de acciones: "Al examinar el análisis de las tradiciones de los Estados miembros en materia de normas de concurrencia, tal como se indica en la jurisprudencia del TJUE, y teniendo en cuenta los diferentes ámbitos de aplicación y las consecuencias jurídicas, estos principios pueden agruparse aproximadamente en las tres categorías siguientes: - Concurrencia de infracciones (capítulo 3.1.1), - Unidad de acción (capítulo 3.1.2), - Pluralidad de acciones (capítulo 3.2).

En los supuestos de concurrencia de infracciones la previsión establecida al respecto es la contenida en el artículo 83.3 del RGPD que establece un límite cuantitativo en estos supuestos de concurrencia: "Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves." (el subrayado es nuestro). (…)

Por último y no menos importante, la AEPD no sanciona por una misma ofensa, como aduce la parte reclamada, sino que se han constatado a través

de hechos probados no rebatidos por TPHS, la comisión de dos infracciones diferenciadas, tipificadas de forma diferenciada, no existiendo, además, en el caso concreto, concurso medial.

Nos encontramos, por lo tanto, ante dos infracciones perfectamente diferencias, que responde a tipos infractores independientemente considerados y, en definitiva, no puede afirmarse que nos encontremos ante un concurso de infracciones.

Alega también la recurrente una contradicción entre lo afirmado por esta AEPD en el sentido de que el art. 83.3 se aplica a la concurrencia de infracciones y que, por lo tanto, no sería de aplicación al caso que nos ocupa en que, como venimos argumentando, no se ha producido tal concurrencia de infracciones y lo que indica el CEPD en sus Directrices 4/2022.

Al respecto cabe recordar que el artículo 83.3 indica lo siguiente:

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

La propia dicción del precepto, al prever como límite máximo la cuantía prevista para las infracciones más graves, parte de la premisa de que las infracciones está vinculadas, como así han de estarlo las sanciones que lleven aparejadas, en el sentido de que el máximo a imponer será el previsto para la más grave de ellas. Es decir, al establecer esta vinculación entre las sanciones - en forma de limitación de la cuantía máxima-, ha de concluirse que las infracciones también han de estarlo y que, por lo tanto, una necesite de la otra, situación que se plantea en los supuestos de concurso medial de infracciones.

En refuerzo de este argumento, cabe destacar la propia jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), señalada, sin ir más lejos, por la recurrente en su recurso.

Así, el apartado 72 de la STJUE de 5 de diciembre de 2023 dictada en el asunto C-683/21, indica lo siguiente (el subrayado es nuestro):

72. Además, es importante leer el artículo 83, apartado 2, del RGPD en relación con el apartado 3 de dicho artículo, cuyo objeto es prever las consecuencias de los casos de acumulación de infracciones del Reglamento y a tenor del cual «si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves»

En casi idénticos términos se pronuncia el apartado 67 de la STJUE de 5 de diciembre de 2023, caso C-807/21.

Por lo tanto, esta alegación ha de desestimarse.

En relación con la alegación relativa a la inadmisibilidad de la responsabilidad objetiva y, como muestra de que la recurrente vuelve a plantear argumentos que ya fueron analizados en la resolución sancionadora, baste comenzar diciendo que, tal y como se señala en la misma (página 199):

> *Vuelve de nuevo a reiterar TPHS esta alegación que ya esgrimió frente al Acuerdo de Inicio, cuya respuesta fue debidamente argumentada en la Propuesta de Resolución y que aparece transcrita en el Antecedente de Hecho Noveno de la presente Resolución, punto Cuarto, a la que, en aras de economía procesal, procede remitirse. En dicha argumentación, ya se indicó la existencia de negligencia en la actuación de TPHS.* (…)
>
> *Así, se indicó que la vulneración de la confidencialidad que se imputa a TPHS es por incumplir la obligación impuesta en el artículo 5.1.f de tratar los datos de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito, mediante la aplicación de medidas técnicas u organizativas apropiadas.*
>
> *No debe olvidarse, en este sentido, que existen medidas dirigidas específicamente a garantizar la confidencialidad de los datos personales, como el cifrado de los mismos o la aplicación sobre ellos de técnicas de pseudonimización o anonimización, medidas que además indicó TPHS expresamente en sus EIPD como medidas necesarias a implantar para reducir los riesgos "altos" o "muy altos" respecto de las actividades de tratamiento afectadas por la brecha. Sin embargo, tal y como se ha indicado en los Hechos Probados, en el momento de producirse el incidente de seguridad, el mismo ha conllevado una brecha de datos personales que ha afectado a la confidencialidad de éstos por cuanto TPHS no había implementado esas medidas concretas tras más de dos años de detectados esos riesgos e indicadas esas medidas en sus EIPD. En caso de haberse aplicado, no se hubiera producido un acceso ni una exfiltración de los datos personales -ni una publicación de los mismos en texto claro- como finalmente sucedió, pues los datos hubieran sido ininteligibles para el delincuente. Esto lo que refleja es, cuanto menos, una falta de la diligencia debida por parte de TPHS.*
>
> *Por tanto, en el supuesto examinado, tal y como consta en los hechos probados, hay una clara pérdida de confidencialidad pues se ha producido el acceso por un tercero no autorizado a los datos personales tratados por TPHS, siendo ello un resultado objetivo, reconocido por TPHS, que no una responsabilidad objetiva. No se ha garantizado, de esta forma, una seguridad adecuada mediante la aplicación de las medidas técnicas y organizativas apropiadas, no sólo de seguridad, sino de todo tipo.*

Frente a lo alegado de nuevo de contrario de que se está imponiendo una responsabilidad objetiva independiente de las medidas desplegadas, no cabe sino recordar lo que razonábamos en la resolución recurrida (página 202):

> *Tal y como se ha venido demostrando y argumentando a lo largo del presente procedimiento sancionador, se considera que no había implantadas unas medidas de seguridad apropiadas para garantizar una seguridad adecuada al riesgo, aunque no hubiera habido brecha de datos personales.*
>
> *Al respecto, esta Agencia desea señalar que de ninguna manera considera que la obligación de implementación de medidas de seguridad impuesta por la normativa de protección de datos tenga una naturaleza de obligación de resultado y no de medios. Pero no es menos cierto que TPHS no contaba, antes de que se produjera el incidente, con medidas que "conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado".*

A diferencia de lo que afirma la recurrente, esta afirmación no encuentra su justificación únicamente en el resultado, sino que, tal y como se indica de forma reiterada, la ausencia de medidas técnicas y organizativas de seguridad ha quedado constatada con independencia o no de que se hubiera producido la pérdida de confidencialidad derivada de la brecha de datos personales.

Señala también la recurrente que el TJUE ya ha concluido que el incremento de obligaciones para el tratamiento de datos personales derivado de la entrada en vigor del RGPD no ha de entenderse como la posibilidad de que la normativa incluya una extensión de la responsabilidad y, muy especialmente, en los requisitos necesarios para poder atribuir consecuencias sancionadoras a la conducta de la persona jurídica. Alude de nuevo a la jurisprudencia del TJUE que ya fue tenida en consideración en la resolución objeto de recurso en los siguientes términos:

> *Por último, añade TPHS que este hecho evidencia claramente que no queda acreditada la concurrencia de una actuación culpable, intencionada o negligente por parte de TPHS no pudiendo, por tanto identificar en su conducta una infracción de la normativa de protección de datos personales por el mero hecho de haber sido víctima de un ciberataque y, consecuentemente, no siendo procedente la imposición ningún tipo de sanción, todo ello teniendo en consideración la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) relativas a los asuntos C-683/21 (Nacionalinis visuomenėssveikatos centras) y C-807/21 (Deutsche Wohnen) publicada el pasado día 5 de diciembre de 2023.*
>
> *Frente a ello, ha quedado acreditado la existencia de deficiencias en las medidas de seguridad aplicadas, así como la ausencia de otras, siendo ello reflejo de una negligencia por parte de TPHS, incurriendo con ello en las infracciones imputadas. Negligencia que es la que exige la sentencia referida para poder sancionar por incumplimientos en las obligaciones que establece el RGPD a los responsables de tratamientos de datos personales.*

A este respecto no cabe sino destacar que la recurrente parte de una premisa equivocada: que, al no considerarse culpable de la conducta que se le imputa, la imposición de una sanción por la misma supone una modificación de las condiciones

materiales para el establecimiento de la responsabilidad. Esta conclusión no puede compartirse.

Así, recordemos que la STJUE dictada en el caso C-683/21 señala lo siguiente:

73 Así pues, del tenor del artículo 83, apartado 2, del RGPD se desprende que únicamente las infracciones de las disposiciones del Reglamento cometidas con culpabilidad por el responsable del tratamiento, a saber, las cometidas de forma intencionada o negligente, pueden dar lugar a que se le imponga una multa administrativa con arreglo a dicho artículo.

80 En consecuencia, procede declarar que el artículo 83 del RGPD no permite imponer una multa administrativa por una infracción contemplada en sus apartados 4 a 6 sin que se demuestre que dicha infracción fue cometida de forma intencionada o negligente por el responsable del tratamiento y que, por lo tanto, la culpabilidad en la comisión de la infracción constituye un requisito para la imposición de la multa.

En idénticos términos se pronuncia la STJUE dictada en el caso C-807/21, apartados 68 y 75, respectivamente.

En definitiva, dichos pronunciamientos se basan en que la culpabilidad de la conducta atribuida al infractor ha de constituir la premisa para la imposición de la multa. Una circunstancia que, como venimos argumentando, se da en el supuesto de hecho que nos ocupa, en que la conducta por la que se sanciona es culpable y deviene de una falta de diligencia claramente demostrada.

Por todo lo anterior, esta alegación ha de ser igualmente desestimada.

En relación a la alegación relativa a las 211 reclamaciones relacionadas con la brecha de seguridad, la recurrente reproduce en este punto, casi en sus exactos términos, las alegaciones vertidas a la propuesta de resolución (página 204 y ss)

> *A este respecto, debe señalarse que TPHS solicitó copia de las citadas reclamaciones en julio de 2022, es decir, mientras se estaban realizando las actuaciones previas de investigación. En ambos casos no se le facilitaron las mismas ya que se le comunicó, por parte de la Subdirección General de Inspección de Datos, que las actuaciones previas de investigación tienen como finalidad lograr una mejor determinación de los hechos y las circunstancias que pudieran justificar, en su caso, la tramitación de un procedimiento sancionador, y no podían tener una duración superior a doce meses. Asimismo, se le comunicó que, una vez concluidas, su resultado se pondría en conocimiento de los interesados, notificándose el archivo de las actuaciones previas de investigación, o bien, el acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*
>
> *Por tanto, a lo largo del procedimiento sancionador no ha sido solicitado de forma expresa por TPHS ni acceso ni copia de las citadas reclamaciones. Lo que se ha pedido por parte de TPHS ha sido copia del expediente sancionador*

que se tramita, la cual le fue debidamente facilitada y del que no forman parte dichas reclamaciones.

No obstante lo anterior, el hecho de que no se hayan incluido en la copia del expediente solicitado -por no estar incluidas en el mismo-, ello no le ha provocado indefensión alguna por cuanto el presente procedimiento sancionador se ha basado en los hechos probados obtenidos durante las actuaciones previas de investigación realizadas y que las mismas no se han centrado en las reclamaciones sino en las investigaciones realizadas con ocasión de la notificación de la brecha de datos personales realizada por TPHS, es decir, en los documentos obtenidos en la misma, fundamentalmente aportados por la propia empresa.
(…) *en el presente caso las actuaciones de investigación no se impulsaron o se iniciaron como consecuencia de las reclamaciones presentadas, sino que fueron consecuencia de la notificación por parte de TPHS de la brecha de datos personales sufrida. Así se indica en la nota interior referida en la que la Directora de esta Agencia dirigió a la Subdirección General de Inspección de Datos con fecha 19 de abril de 2021 ordenando que valorase la necesidad de realizar las oportunas investigaciones previas Y esa es la fecha que se tiene en cuenta para el inicio del cómputo de las actuaciones de investigación las cuales, tras doce meses, se declaró su caducidad el 19 de abril de 2022 y el inicio de unas nuevas actuaciones de investigación.*

Asimismo, las nuevas actuaciones de investigación se abrieron al objeto de poder proseguir con las mismas, en concreto para poder solicitar aclaración sobre algunos extremos así como recabar evidencias respecto de varios aspectos (…)

Cabe aclarar por otro lado que la indicación de que a estos reclamantes se les comunicará la existencia de la resolución finalizadora del procedimiento sancionador no significa que sus reclamaciones hayan sido tenidas en cuenta o que su desconocimiento por la recurrente le haya causado indefensión, como insiste en afirmar, sino que trae causa de lo dispuesto en la LPACAP

- En el artículo 4. Concepto de interesado

  1. Se consideran interesados en el procedimiento administrativo:

  b) Los que, sin haber iniciado el procedimiento, tengan derechos que puedan resultar afectados por la decisión que en el mismo se adopte.(…)

- En el artículo 40. Notificación.

  1. El órgano que dicte las resoluciones y actos administrativos los notificará a los interesados cuyos derechos e intereses sean afectados por aquéllos, en los términos previstos en los artículos siguientes.(…)

Esta alegación ha de desestimarse.

Contiene a continuación el recurso alegaciones relativas a la prueba, ya que la recurrente califica de parcial y diferenciada la valoración de la prueba realizada por la AEPD. De nuevo, parece confundir la diferencia de criterio en cuanto a la necesidad de practicar determinada prueba con una falta de rigor en su valoración.

Insiste de nuevo en el valor probatorio del informe adicional SIA presentado; un documento que, reiteramos, ha sido tomado en consideración pero que, a diferencia de lo que insiste en plantear la recurrente, no puede desvirtuar las conclusiones por el resto de documentos y hallazgos que conforman el expediente y con base a los cuales ha sido dictada la resolución sancionadora. Tal y como se le ha indicado repetidamente, el denominado "informe aclaratorio SIA" ha sido debidamente analizado y valorado, un análisis y valoración que no ha permitido alcanzar conclusiones que desvirtúen que se han cometido las conductas infractoras que se sancionan

En definitiva, se desestima esta alegación.

Sobre la ausencia de proporcionalidad en la fijación de la cuantía de la sanción impuesta no cabe sino remitirnos, de nuevo, a lo ya razonado en la resolución recurrida:

Página 208

> *En primer lugar, y en contra de la interpretación que hace TPHS sobre los límites de los importes de las multas, ya se explicó y argumentó cómo establece el RGPD dichos límites en la respuesta que se dio a esta alegación en la Propuesta de Resolución y que se transcribe en el Antecedente de Hecho Noveno, punto Décimo, al cual procede remitirse.*
>
> *Así, se señaló, en primer lugar, que el artículo 83.1 RGPD establece que las multas administrativas por las infracciones del RGPD deben ser "…en cada caso individual efectivas, proporcionadas y disuasorias", indicando a continuación en el apartado 2 del citado precepto, que "Las multas administrativas se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas…" (el subrayado es nuestro). Estableciendo a continuación determinadas circunstancias a tener en cuenta.*
> (…)
>
> *En segundo lugar, en cuanto al límite máximo, a TPHS se le imputan dos infracciones: una por infringir el artículo 5.1.f) RGPD y otra por infringir el artículo 32 RGPD, infracciones que vienen, a su vez, tipificadas en el artículo 83.5 y 83.4 respectivamente.*
>
> *A este respecto, el artículo 83.5 RGPD señala que las infracciones de las disposiciones que indica "…se sancionarán 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 del negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía" (el subrayado es nuestro).*

Asimismo, el artículo 83.4 señala que las infracciones de las disposiciones que indica "…se sancionarán 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 del negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía" (el subrayado es nuestro).

Es decir, los porcentajes sobre el volumen de negocio, cuando se trata de una empresa, no operan como límites máximos cuando la cifra que arrojan es menor a 10 ó 20 millones -según estemos en la tipificación del apartado 4 ó 5 del artículo 83 RGPD respectivamente-, sino todo lo contrario, permiten obtener un límite máximo superior a esos 10 ó 20 millones.

Por tanto, cuando el 2% ó el 4% del volumen de negocio total anual global de la multa impuesta para cada infracción sea menor a los importes máximos establecidos en los citados preceptos, 10 ó 20 millones de euros, éstos últimos serán los límites máximos. Por el contrario, si esos porcentajes arrojan importes superiores, serán los tenidos en cuenta como límites máximos. Y ello porque el RGPD establece que ha de optarse por la de mayor cuantía. (…)

En el presente caso, se han tenido en cuenta las circunstancias del caso: la gravedad de las infracciones, las consecuencias de las mismas, la falta de diligencia mostrada, los concretos tratamientos que realiza, la tipología de datos personales y el número de personas afectadas, las circunstancias de la empresa (tamaño, volumen de negocio, etc.), circunstancias todas ellas puestas de manifiesto y motivadas en el Acuerdo de Inicio del presente procedimiento sancionador y que se reproducen en los Fundamentos de Derecho VI y IX de la presente Resolución, a la que nos remitimos, las cuales permiten concluir que se ha respetado el principio de proporcionalidad a la hora de determinar la cuantía de las multas finalmente impuestas.

Por tanto, a la hora de determinar la cuantía de las multas no sólo se tiene en cuenta el nivel de negocio de las empresas. Ello es una circunstancia más. También se tienen en cuenta, como se ha señalado, otras circunstancias, especialmente las circunstancias específicas de cada caso (lo que ha sucedido, los efectos o repercusión para los datos personales, número de afectados, nivel de negligencia, etc). En el expediente que trae a colación TPHS, las circunstancias son muy diferentes y, a modo de ejemplo, en el referido EXP202204846, se confirmó la vulneración de la confidencialidad de los datos personales de 760 personas y potencialmente de millones (pero no acreditado). Mientras que en el caso que nos ocupa consta acreditado que se ha vulnerado la confidencialidad de los datos personales de 13 millones de personas, constituyendo ello desde el punto de vista del número de personas afectadas, uno de los episodios de exfiltración de datos personales más importantes, sino el que más, sucedido en nuestro país.

Volvemos a traer a colación lo manifestado por el TJUE en la sentencia dictada en el asunto C-683-21

78 La existencia de un sistema de sanciones que permita imponer, cuando las circunstancias específicas de cada caso lo justifiquen, una multa administrativa con arreglo al artículo 83 del RGPD crea un incentivo para que los responsables y encargados del tratamiento cumplan el Reglamento. Con su efecto disuasorio, las multas administrativas contribuyen a reforzar la protección de las personas físicas en lo que respecta al tratamiento de datos personales y constituyen, por ende, un elemento clave para garantizar el respeto de los derechos de dichas personas, de conformidad con la finalidad del citado Reglamento de asegurar un elevado nivel de protección de esas personas en lo que respecta al tratamiento de los datos personales.

En idéntico sentido, el apartado 73 de la STJUE dictada en el caso C-807/21

Cuestiona también la recurrente el número de afectados reflejados en la resolución y alega que la cifra de 13 millones se corresponde con sus usuarios y clientes, *pero no consta acreditado de forma alguna que sea esa la cifra de interesados cuyos datos se han visto afectados.* No puede compartirse esta apreciación dado que, como ha quedado constatado en el expediente, ha sido la propia recurrente la que identificó esa cifra como la del número de afectados.

(Página 91)

> *En cuanto al número de interesados afectados, no puede obviarse que es altísimo: 13.000.000 de afectados. Es una cifra que no ofrece dudas. A este respecto, en cuanto a lo aducido por TPHS respecto de que esta Agencia realiza una valoración subjetiva del volumen de afectados y que su número es una mera aproximación o estimación no contrastada, procede señalar que fue la propia compañía la que, al notificar a esta Agencia la brecha de datos personales, en su escrito presentado el 28 de abril de 2021 (nº registro O00007128e2100019496), señaló en el apartado "Número aproximado de registros de datos personales afectados: 13000000".*
>
> *Adjunto a dicha notificación, TPHS aportó el documento "Informe de Evaluación de Brecha de Seguridad", en cuya página 18 indica "Número aproximado de personas afectadas:13.000.000".*
>
> *Asimismo, en el "Informe de análisis de incidente ransomware" elaborado por la empresa SIA Group, contratada por TPHS para el análisis de lo ocurrido y fechada el 21 de abril de 2021, y aportada por la misma al expediente, se indica, en las "Conclusiones" que, en relación con las publicaciones realizadas por el ciberdelincuente, indica que "Finalmente, el martes 20 de abril de 2021 publica en otro dominio de la red TOR dos ficheros de alrededor de 1 GB de tamaño con datos de carácter personal de 13 millones de personas"*
>
> *Por tanto, no puede aceptarse que sea una apreciación subjetiva de esta Agencia sin sustento alguno el considerar que se vieron afectados un número muy elevado de interesados (la cantidad de 13 millones por sí sola es suficiente para tal consideración), así como que tampoco esté contrastado el*

número de afectados, pues el mismo ha sido indicado por la propia empresa, además de venir indicado también en el informe realizado por la empresa experta en ciberseguridad y contratada por TPHS precisamente para analizar el incidente ocurrido.

No cabe, por lo tanto, cuestionar la veracidad de un dato que fue ofrecido por la propia recurrente y que, como tal, tuvo su reflejo en la resolución que se recurre.

Concluimos, por lo tanto, que la sanción impuesta proporcional a la infracción cometida y a las consecuencias de la misma, de acuerdo con el espíritu y criterios objetivos fijados por el RGPD, ***(…).***

Por lo anteriormente expuesto, esta alegación se desestima.

En relación a la alegación relativa a los agravantes asociados por la AEPD a las infracciones, la recurrente señala cuestiona las circunstancias que se han tenido en cuenta como agravantes, mostrando su disconformidad, con unos argumentos de nuevo coincidentes con los ya planteados durante el procedimiento sancionador:

1) Naturaleza y gravedad de la infracción (artículo 83.2 a) RGPD). Entiende la recurrente que el número de afectados por la brecha no ha quedado confirmado y no se concreta en la resolución. Al respecto, procede remitirnos a lo indicado con carácter previo a que la cifra de 13 millones de personas proviene de la información precisamente proporcionada por la recurrente.

2) En cuando al nivel de daños y perjuicios sufridos, entiende que no consta prueba alguna que los datos afectados por la brecha se han publicado en la Deep web

A este respecto, nos remitimos a lo señalado por la resolución, en su página 5

> *Con fecha 28 de abril de 2021, TPHS presenta nueva notificación (en adelante Notificación2) ampliando la información sobre la brecha de seguridad notificada el 14 del mismo mes, en el que indican que,* ***(…).***

Así como en la página 12

> *En el Informe28A manifiesta el investigado que, de las investigaciones realizadas, se han concluido las siguientes afectaciones del ataque:*
>
> ***(…).***

O en la página 38

> *Concluye por tanto que, en relación con la confidencialidad, debe tenerse en cuenta que una vez esta se ha visto vulnerada por un ataque que produce una brecha de seguridad, la subsiguiente actuación ilícita*

por parte de los ciberdelincuentes, consistente en la publicación en la Deep Web de la información, es un hecho independiente y no atribuible a la Compañía, dado que no tiene ninguna capacidad para impedirlo.

Por lo tanto, puede afirmarse que la publicación de los datos en la Deep web ha quedado acreditada.

Cabe igualmente recordar lo señalado en la página 212 de la resolución recurrida en el sentido siguiente:

Así, no se le imputa la publicación en la Deep Web de los datos personales, sino que ello se menciona como factor de acreditación de que se vulneró la confidencialidad y de que los datos aparecieron en texto claro. La vulneración de la confidencialidad que se imputa a TPHS es la que le corresponde, es decir, por incumplir la obligación impuesta en el artículo 5.1.f de tratar los datos de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Procede recordar, en este sentido, que existen medidas dirigidas específicamente a garantizar la confidencialidad de los datos personales, como el cifrado de los mismos o la aplicación sobre ellos de técnicas de pseudonimización o anonimización, medidas que además indicó expresamente en sus EIPD respecto de las actividades de tratamiento afectadas por la brecha. En caso de haberse aplicado, no se hubiera producido un acceso por un tercero no autorizado a los datos personales ni, en consecuencia, la publicación ulterior de los mismos. Y ello porque la pérdida de confidencialidad se constató como consecuencia de la exfiltración de los datos; pérdida de confidencialidad, acceso de un tercero a los datos personales, que no se hubiera producido si estos hubieran estado cifrados o pseudonimizados o anonimizados, pues los delincuentes se hubieran llevado una información ininteligible.

A este respecto, procede traer a colación de nuevo la Sentencia de 22 de junio de 2021- Rec. 1210/2018, y la Sentencia de 5 de noviembre de 2011 -Rec. 1796/2019 en la cual la Sala valorando el elemento subjetivo o culpabilístico "…insistiendo en que la culpabilidad de la parte actora no puede considerarse excluida ni atenuada por el hecho de que haya mediado la posible actuación fraudulenta de un tercero, pues la responsabilidad de la parte actora no deriva de la actuación de éste, sino de la suya propia".

3) Duración de la infracción

Basa la recurrente sus alegaciones en relación con esta circunstancia al reiterado argumento de que los sistemas de información identificados en las EIPD cuyas medidas no fueron adoptadas, hecho que se tiene en cuenta para la graduación de la sanción, no están relacionados con la brecha sufrida. A este

respecto, y por economía procesal, nos remitimos a los argumentos señalados previamente.

4) Intencionalidad o negligencia en la infracción

Como ya ha quedado de manifiesto a lo largo de la tramitación de todo el procedimiento sancionador, ha quedado constatada la conducta culpable atribuible a la parte recurrente cuya respuesta jurídica se contiene en la resolución recurrida. Cabe recordar que, según lo que señalamos en la página 213.

> *En cuanto a la falta de negligencia alegada, se significa que se ha argumentado perfectamente la consideración de la existencia de la misma a lo largo de todo el procedimiento sancionador, tanto en el Acuerdo de Inicio como en la Propuesta de Resolución, pues la ausencia de determinadas medidas, así como las deficiencias en otras, refleja una clara falta del deber de diligencia que se le debe exigir a una empresa con la naturaleza de tratamientos de datos que realiza, así como por el carácter masivo de éstos.*

Y ello, sin que quepa aceptar que la condición de víctima o perjudicada por el ciberataque permita eludir su responsabilidad en la falta de medidas que hubiesen podido siquiera mitigar las consecuencias de la brecha de datos personales.

5) Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal

Alega la recurrente que su actividad no puede ser considerada, de manera genérica, como agravante y señala que las Directrices 4/2022 antes mencionadas excluye la actividad y sector empresarial concreto del infractor como criterio a considerar en la imposición y cuantificación de sanciones por la infracción de la normativa de protección de datos.

Parece obviar la recurrente el hecho de que la circunstancia que se tiene en consideración no es la actividad que desempeña en sí misma considerada, sino el hecho claro de que, en su ejecución, realiza un tratamiento masivo de datos personales. Y es palmario que, al tratarse de una empresa habituada al tratamiento de datos personales, su exigencia de diligencia ha de ser mayor.

En definitiva, como se argumentaba en la resolución recurrida:

> *Cabe destacar que no puede tener a los efectos de decidir la imposición de una multa administrativa, la misma consideración una infracción producida por una persona física o una empresa pequeña no habituada al tratamiento de datos personales, que una gran empresa como TPHS, acostumbrada al tratamiento de datos personales de millones de clientes y no clientes, con una larga trayectoria a sus espaldas al respecto. Por supuesto que se considera que la infracción es más grave*

> *a los efectos de imponer una multa si el responsable del tratamiento se encuentra entre los segundos, como es el caso de TPHS.*

Con base en lo anteriormente razonado, esta alegación también ha de ser desestimada.

Realiza a continuación la recurrente alegaciones sobre la concurrencia de factores atenuantes no considerados

Alega la recurrente que actuó de manera diligente, adoptando las medidas necesarias para mitigar sus efectos y reforzar la seguridad de sus sistemas. Señala también que esta atenuante fue aplicada en el expediente con referencia EXP202204846.

A lo anterior tan sólo cabe reiterar que, en el presente caso, se han tenido en cuenta las circunstancias del caso: la gravedad de las infracciones, las consecuencias de las mismas, la falta de diligencia mostrada, los concretos tratamientos que realiza, la tipología de datos personales y el número de personas afectadas, las circunstancias de la empresa (tamaño, volumen de negocio, etc.),

Como razonábamos en la resolución sancionadora (página 210)

> *Por tanto, a la hora de determinar la cuantía de las multas no sólo se tiene en cuenta el nivel de negocio de las empresas. Ello es una circunstancia más. También se tienen en cuenta, como se ha señalado, otras circunstancias, especialmente las circunstancias específicas de cada caso (lo que ha sucedido, los efectos o repercusión para los datos personales, número de afectados, nivel de negligencia, etc). En el expediente que trae a colación TPHS, las circunstancias son muy diferentes y, a modo de ejemplo, en el referido EXP202204846, se confirmó la vulneración de la confidencialidad de los datos personales de 760 personas y potencialmente de millones (pero no acreditado). Mientras que en el caso que nos ocupa consta acreditado que se ha vulnerado la confidencialidad de los datos personales de 13 millones de personas, constituyendo ello* desde el punto de vista del número de personas afectadas, uno de los episodios de exfiltración de datos personales más importantes, sino el que más, sucedido en nuestro país.
>
> *Asimismo, la ausencia de medidas adecuadas y las deficiencias detectadas en otras ha puesto de manifiesto una importante negligencia por parte de TPHS, medidas de seguridad conocidas, básicas y al alcance de una empresa de su tamaño y con los tratamientos masivos que realiza de millones de personas.*

Por todo lo anterior, esta alegación también ha de desestimarse.

Realiza finalmente la recurrente una serie de consideraciones respecto a las medidas impuestas en la resolución sancionadora. Entiende que sus tratamientos ya estaban adecuados a la normativa en el momento en que se produjeron los hechos y aporta documentación relacionada con las medidas adoptadas (Documento nº2), el listado de empleados que realizaron la formación en protección de datos en 2023 (Documento nº 3), un video explicativo del origen del listado (Documento nº 4) y actualiza el número de trabajadores de la empresa a fecha del escrito de recurso. A este respecto, tan sólo

cabría señalar que cualquier consideración relacionada con las medidas indicadas en la resolución recurrida debe hacerse de acuerdo con lo señalado en la misma; en concreto en el apartado tercero de la parte dispositiva, en el que se señala lo siguiente:

> *TERCERO: ORDENAR a THE PHONE HOUSE SPAIN, S.L. con NIF B81846206, que en virtud del artículo 58.2.d) del RGPD, en el plazo de seis meses, notifique a la Agencia la adopción de las medidas a la vista del contenido del fundamento de derecho X.*

III
Conclusión

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada, por lo que no pueden aceptarse las alegaciones presentadas y ha de concluirse con la desestimación del recurso presentado.

IV
Resolución extemporánea

Debido a razones de funcionamiento del órgano administrativo, por ende no atribuibles a la parte recurrente, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de esta Agencia respecto al presente recurso.

De acuerdo con lo establecido en el art. 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el art. 21.1 de la citada LPACAP.

Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

Vistos los preceptos citados y demás de general aplicación, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **THE PHONE HOUSE SPAIN, S.L.** contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 27 de diciembre de 2023, en el expediente EXP202306260.

SEGUNDO: NOTIFICAR la presente resolución a **THE PHONE HOUSE SPAIN, S.L.**.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea notificada la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo

Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Si la fecha de la notificación se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer 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) 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 LPACAP. 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.

180-21112023

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