- **Expediente N.º: EXP202205206**

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

índice

ANTECEDENTES

PRIMERO: Con fecha 18 de marzo de 2022 se notificó a la División de Innovación Tecnológica de esta Agencia Española de Protección de Datos (en adelante AEPD o la Agencia) una brecha de seguridad de los datos personales remitido por I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U. con NIF A95075578 (en adelante, I-DE) como responsable del tratamiento, en la que informa a esta Agencia de lo siguiente:

El 15 de marzo de 2022 por la tarde, se detecta un ataque contra la web de gestión de acometidas (GEA) de I-DE. ***(...)***. En este momento aún no se identifica afección a datos personales. Al día siguiente, 16 de marzo, se detecta un ataque de fuerza bruta dirigido contra el mismo objetivo (GEA) que el incidente del día anterior. Se repele adoptando medidas. El 17 de marzo se reabre GEA se analiza el registro de actividad y se concluye que ha habido extracción de datos personales. Se indica que el número de afectados es de 4,5 millones de clientes de esta sociedad.

SEGUNDO: Con fecha 29 de marzo de 2022, I-DE presenta nueva notificación ampliando la información sobre la brecha de seguridad notificada el 18 del mismo mes, en el que indica que, tras el análisis forense del incidente, el número de sus clientes cuyos datos han sido afectados son 1,35 millones y que también es probable la existencia de datos afectados de clientes de otras sociedades del grupo Iberdrola, ya que el atacante, potencialmente podría haber superado las condiciones de seguridad de la información exclusiva de I-DE, saltando a rangos de información de otras sociedades, lo cual ya ha sido transmitido a la dirección de Sistemas de la Compañía para un análisis detallado de otras afecciones en otras sociedades o negocios del grupo Iberdrola.

Asimismo, indican que la fecha exacta de inicio de la brecha es el 7 de marzo de 2022 e informan de que todavía no se ha comunicado la brecha a las personas afectadas y que, a más tardar, serán informadas el 31 de marzo de 2022.

Junto a la notificación se aporta:

- Informe “Incidente ciber GEA. Descripción incidente y acciones”, en el que describe el ataque sufrido y que incluye, además, el texto de la comunicación que se va a remitir a los afectados.

TERCERO: con fecha 29 de marzo de 2022, CURENERGIA COMERCIALIZADOR DE ULTIMO RECURSO SA, con N.I.F. A95554630 (en adelante CURENERGÍA) presenta notificación de brecha de seguridad, en la que indica que ha tenido constancia el 28 de marzo de 2022 de que ha sido afectada por la brecha de seguridad sufrida por I-DE, indicando la vulneración de la confidencialidad de los datos personales de 1.550.000 de sus clientes, a los cuales aún no ha informado pero que lo hará a más tardar el 31/03/2022.

CUARTO: con fecha con fecha 28 de marzo de 2022, IBERDROLA CLIENTES, S.A., con N.I.F. A95758389 (en adelante IBERCLI) presenta notificación de brecha de seguridad, en la que indica que ha tenido constancia el 28 de marzo de 2022 de que ha sido afectada por la brecha de seguridad sufrida por I-DE, indicando la vulneración de la confidencialidad de los datos personales de 85.000 de sus clientes, a los cuales aún no ha informado pero que lo hará a más tardar el 31/03/2022.

QUINTO: Desde el 2 de abril de 2022, se han presentado ante esta Agencia reclamaciones de clientes afectados por el incidente de seguridad, las cuales han sido progresivamente admitidas a trámite desde el 9 de mayo de 2022.

SEXTO: Con fecha 6 de abril de 2022, IBERCLI presenta ampliación de la notificación de brecha en la que informa que las personas afectadas por la misma son 1.515.000 y que se les ha informado de la misma el 31 de marzo de 2022 mediante comunicación dirigida personalmente a cada afectado (postal, mail, sms o similar).

Junto a la notificación se aporta:

- Informe “Incidente ciberataque 28/03/2022. Descripción incidente y acciones”
- Anexo Comunicación a interesados

SÉPTIMO: Con fecha 6 de abril de 2022, CURENERGÍA presenta ampliación de la notificación de brecha en la que informa que las personas afectadas por la misma son 92.550 y que se les ha informado de la misma el 31 de marzo de 2022 mediante comunicación dirigida personalmente a cada afectado (postal, mail, sms o similar).

Junto a la notificación se aporta:

- Informe “Incidente ciberataque 28/03/2022. Descripción incidente y acciones”

- Anexo Comunicación a interesados

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

Durante las presentes actuaciones se han investigado las siguientes entidades:

- I-DE REDES ELECTRICAS INTELIGENTES S.A. con NIF A95075578 (en adelante, I-DE)

- IBERDROLA S.A. con NIF A48010615 con domicilio en C/ TOMAS REDONDO, 1 - 28033 MADRID (MADRID) (en adelante IBERDROLA)

- IBERDROLA CLIENTES S.A.U. con NIF A95758389 (en adelante, IBERCLI)

- CURENERGIA COMERCIALIZADOR DE ULTIMO RECURSO S.A. con NIF A95554630 (en adelante, CURENERGIA)

Marco normativo

- La normativa reguladora del sector eléctrico, *Ley 54/1997, de 27 de noviembre, del Sector Eléctrico*, impone una obligación de separación total entre las actividades reguladas, como es la de distribución, y las liberalizadas, como es la comercialización.

- El derecho que tienen los consumidores de energía eléctrica al acceso y conexión a las redes de transporte y distribución de energía eléctrica en el territorio español se recoge específicamente en la *Ley 24/2013, de 26 de diciembre, del Sector Eléctrico*.

  Las empresas distribuidoras y las empresas comercializadoras son dos entidades diferenciadas en el ámbito del Sector Eléctrico. En este sentido la *Ley 24/2013, de 26 de diciembre, del Sector Eléctrico* las define como sujetos distintos.

- Conforme a la regulación del sector eléctrico, el consumidor, para recibir energía eléctrica en su domicilio, necesita ser titular de dos contratos diferenciados con relación a su punto de suministro (CUPS):

  - Por una parte, el contrato de compra de energía, "*contrato de suministro*", que se suscribe entre un consumidor y una empresa comercializadora de electricidad.

Aunque también cabe la posibilidad de que el consumidor adquiera la electricidad directamente en el mercado, sin necesidad de comercializador, no es propio de los clientes personas físicas sino de empresas grandes consumidoras de electricidad, indican I-DE, IBERCLI y CURENERGÍA en su respuesta.

- Por otra, el contrato de acceso a la red o distribución o transporte, "*contrato de ATR*", que el consumidor suscribe con la intermediación como mandatario de la empresa comercializadora con la que tiene contratada la compra de energía eléctrica.
  Aunque también se puede suscribir directamente con la empresa titular de la red, no es propio de los clientes personas físicas sino de empresas grandes consumidoras de electricidad, indican I-DE, IBERCLI y CURENERGÍA en su respuesta.

- Cuando un cliente desea contratar la electricidad en un punto de suministro o realizar cualquier modificación contractual, dicho cliente acude a una comercializadora, quien en nombre del cliente y como mandatario suyo contrata en su nombre el contrato de ATR, contrato de acceso a la red de distribución.

  Cualquier modificación contractual que solicita un comercializador a un distribuidor se realiza mediante solicitudes digitales XML cumpliendo los formatos de intercambio entre agentes establecidos por la Comisión Nacional de los Mercados y la Competencia (CNMC), en virtud de la *Resolución de 20 de diciembre de 2016, por la que se aprueban los formatos de los ficheros de intercambio de información entre distribuidores y comercializadores de energía eléctrica y de gas natural*, y *Resolución de 17 de diciembre de 2019, por la que se aprueban nuevos formatos de los ficheros de intercambio de información entre distribuidores y comercializadores y se modifica la Resolución de 20 de diciembre de 2016*.

Teniendo en cuenta lo anterior:

- I-DE, distribuidora de energía eléctrica del grupo Iberdrola, manifiesta que únicamente puede acceder a los datos de sus clientes, es decir, de los usuarios del servicio eléctrico cuyo punto de suministro se encuentra dentro de la red cuya gestión, como distribuidora, le corresponde y no a los gestionados por otras empresas distribuidoras.

  En relación con los usuarios de su red, conoce el dato de la comercializadora de cada consumidor como consecuencia de la firma con el mismo (o con la comercializadora como mandataria del consumidor) del contrato de ATR.

- I-DE indica que no tendría capacidad para conocer ningún tipo de información relacionada con quienes siendo clientes de IBERCLI o de CURENERGIA, comercializadoras de energía eléctrica del grupo Iberdrola en el mercado libre y mercado regulado, respectivamente, no lo fueran de esta distribuidora.

Arquitectura de sistemas y base de datos. Aplicación GEA

(…)

IBERDROLA indica que la auditoría de verificación de la separación lógica de los accesos a la información por parte de I-DE trae su causa en lo establecido en la normativa reguladora del sector eléctrico, que impone una obligación de separación total entre las actividades reguladas, como la de distribución y las liberalizadas, como es la comercialización, de forma que las empresas distribuidoras deberán acreditar la citada separación.

I-DE traslada que, anualmente, emite un informe que se presenta ante el Ministerio para la Transición Ecológica y el Reto Demográfico (MITERD) y la Comisión Nacional de los Mercados y la Competencia (CNMC) para dar cuenta del cumplimiento de las obligaciones en materia de separación de actividades por parte de las sociedad del grupo formado por Iberdrola España y las sociedades participadas por esta con actividades reguladas, esto es, la sociedad I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U., artículo 12.2 b) de la Ley del Sector Eléctrico y artículo 14 del Código de separación de Actividades de las Sociedades del Grupo Iberdrola España con Actividades Reguladas (“CSA”) disponible en la página web de Iberdrola España, durante el ejercicio.

(…)

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final.

I-D manifiesta lo siguiente:

- El 15 de marzo, por la tarde, se detectó un ataque contra la web de gestión de acometidas de I-DE, (GEA), siendo la secuencia de los hechos la siguiente:
    - ***(…)***
- El 16 de marzo de 2022, por la mañana, se produce una ralentización general del acceso a varias webs del grupo Iberdrola.
    - ***(…)***
- A partir del día 17 de marzo de 2022:
    - ***(…)***
    - A partir del día 17 no se observa tráfico sospechoso ni afectación en ninguno de los sistemas de servicios en internet del grupo Iberdrola.
    - Del análisis del registro de actividad de la aplicación GEA de los últimos días se concluye con fecha 17 de marzo que se ha producido una exfiltración, entre los días 7 y 15 de marzo de 2022, de aproximadamente 4,5 millones de interesados (personas físicas).
    - ***(…)***
    - En fecha 28 de marzo de 2022, la Dirección de Sistemas comunica a IBERCLI y CURENERGIA la existencia de un incidente de seguridad en

los sistemas de I-DE que ha podido afectar a la información referida a los clientes de estas compañías y les incluye información referida a los códigos internos de cliente de los afectados, a fin de que las compañías verifiquen si han podido verse comprometidos datos correspondientes a sus clientes. Analizada la información por IBERCLI y CURENERGIA verifican que la brecha de seguridad ha afectado a datos personales de clientes de dichas sociedades.

- ***(…)***

- Asimismo, I-DE manifiesta y acredita que desde que tuvo conocimiento del incidente se pusieron en práctica las acciones necesarias para, en coordinación con las organizaciones afectadas, dar cumplimiento a los protocolos internos establecidos a tal efecto y la legislación aplicable, y que incluyen las siguientes acciones:

    - Comunicación al INCIBE-CERT, Instituto Nacional de Ciberseguridad en España, como equipo de respuesta a incidentes de seguridad informática de referencia Iberdrola.
    - Comunicación a la Oficina de Coordinación Cibernética, en virtud del RDL 12/2018 de seguridad de las redes y sistemas de información que remite el incidente de ciberseguridad a la Policía Nacional para investigación,
    - Comunicación al Centro Nacional de Protección de Infraestructuras Críticas en virtud de la Ley 08/2011 de protección de Infraestructuras Críticas.
    - Presentación de una denuncia ante la Policía Nacional (Unidad Central de Ciberdelincuencia) y el documento presentado por I-DE junto con la misma.
    - Notificación de la brecha de seguridad a la AEPD y a los afectados.

- En resumen, los sistemas de monitorización permitieron la detección de un volumen anómalo de tráfico, se puso en marcha una actividad de análisis de mayor detalle y las medidas inmediatas que se adoptaron fueron:

    - ***(…)***

-IBERCLI y CURENERGIA manifiestan que la cesación del incidente se produjo incluso con anterioridad a que tuvieran conocimiento de que aquel había afectado a datos personales referidos a sus clientes, siendo consecuencia dicho cese de las medidas adicionales de seguridad implementadas por la Dirección de Sistemas en el aplicativo GEA, tendentes a impedir que, a partir de un acceso al mismo pudiera exfiltrarse mediante la introducción de un código aleatorio información de la Base de Datos referida a clientes de otras entidades del Grupo.

Respecto de las causas que hicieron posible la brecha

- (…)

Respecto de los datos afectados

- Los datos de los clientes exfiltrados ***(…)***:

    - Nombre
    - Apellidos
    - E-mail
    - Fax
    - Teléfono
    - Dirección
    - NIF/DNI
    - Código Cliente
    - ***(…).***

- ***(…)***

    En fecha 28 de marzo de 2022, la Dirección de Sistemas comunica a IBERCLI y CURENERGIA la existencia de un incidente de seguridad en los sistemas de I-DE que ha podido afectar a la información referida a los clientes de estas compañías y les incluye información referida a los códigos internos de cliente de los afectados, a fin de que las compañías verifiquen si han podido verse comprometidos datos correspondientes a sus clientes.
    IBERCLI y CURENERGÍA verifican que la brecha de seguridad ha afectado a datos personales de 1.515.000 y 92.550 clientes, respectivamente.

Respecto del contrato de encargado del tratamiento

- Se aporta el *Acuerdo Marco de Protección de Datos Personales del Grupo Iberdrola* en el que se detalla el alcance de la prestación de servicios a las empresas del Grupo llevada a cabo por IBERDROLA. Este acuerdo ha sido actualizado en su Anexo II, estando dicha actualización pendiente de formalización.

    Asimismo, se aporta la *Declaración de Aceptación de Iberdrola España S.A.U. de su adhesión al Acuerdo Marco de Protección de Datos Personales del Grupo Iberdrola*, actuando la citada entidad, conforme a lo indicado en la cláusula segunda, en su propio nombre y derecho y en representación de las sociedades pertenecientes a su grupo societario sobre las que ostenta directa o indirectamente el control, entre las que se encuentran I-DE, IBERCLI y CURENERGIA.

- IBERCLI y CURENERGIA aportan copia del registro de las actividades de tratamiento de datos personales correspondientes a los tratamientos afectados por la brecha:

    - ***(…)***

- IBERDROLA aporta copia de los registros de las actividades de tratamiento correspondientes a los tratamientos "*Soporte y Mantenimiento de*

Infraestructuras IT" y *"Desarrollo de aplicaciones (SWF)"*, que lleva a cabo en su condición de encargada del tratamiento, respecto de diversos tratamientos de las sociedades del Grupo, entre los que se encuentran los afectados por la brecha de seguridad.

Respecto de las medidas de seguridad

Respecto del análisis de riesgos realizado sobre la actividad del tratamiento que ha sufrido la brecha de seguridad con anterioridad a que se produjera la brecha:

- IBERDROLA manifiesta en escrito de respuesta, que el Grupo Iberdrola ha adoptado una metodología de análisis de riesgo de los tratamientos de datos personales que se encuentra implantada de forma automatizada en la propia herramienta corporativa de registro de actividades de tratamiento, de forma que en el propio proceso de registro se determina el nivel de riesgo del tratamiento.

- En el caso de los tratamientos respecto de los que IBERDROLA actúa como encargado del tratamiento, señala que la metodología implica la realización del análisis de riesgos en relación con cada uno de los tratamientos respecto de los que IBERDROLA ostenta dicha condición, de forma que ese análisis se desarrolla por la propia entidad responsable del tratamiento en colaboración con IBERDROLA

- Por este motivo, el resultado del análisis de riesgos relacionado con los específicos tratamientos ******TRATAMIENTO.1 y ***TRATAMIENTO.2*** figura incorporado a los Registros de Actividades de Tratamiento de I-DE y a los de IBERCLI y CURENERGIA, habiendo sido comunicado sus resultados a IBERDROLA.

(…)

-Medidas de seguridad implantadas con anterioridad a la brecha en los tratamientos de datos donde se ha producido:

I-DE, IBERCLI y CURENERGIA indican en sus respuestas que con anterioridad a la incidencia se encontraban implantadas las siguientes medidas de seguridad comunes a la infraestructura TI del Grupo Iberdrola:

- ***(…)***

Asimismo, al igual que IBERDROLA, describen también las medidas de seguridad específicas del sistema GEA:

- ***(…)***

Medidas adoptadas para evitar, en lo posible, incidentes como el sucedido

- Con los datos obtenidos de la metodología del ciberataque, ***(…).***

Respecto de la comunicación a los afectados

- I-DE comunica a la Dirección de Sistemas, en fecha 28 de marzo de 2022, que, de la información facilitada referida a los códigos de cliente de los afectados por la brecha, únicamente 1,34 millones de registros se corresponden con clientes de I-DE.

Asimismo, determina que procederá a comunicar la brecha de seguridad a los afectados a través de los canales de comunicación que I-DE mantiene con los mismos. Las comunicaciones fueron remitidas a través de correo electrónico; a los clientes de los que disponía de la dirección de correo electrónico, mediante la realización de varios envíos entre los días 31 de marzo y 12 de abril de 2022; y por correo postal a los restantes entre los días 30 de marzo y 7 de abril de 2022.

- En fecha 28 de marzo de 2022, la Dirección de Sistemas comunica a IBERCLI y CURENERGIA la existencia de un incidente de seguridad en los sistemas de I-DE que ha podido afectar a la información referida a los clientes de estas compañías y les incluye información referida a los códigos internos de cliente de los afectados, a fin de que las compañías verifiquen si han podido verse comprometidos datos correspondientes a sus clientes.

IBERCLI y CURENERGÍA trasladan que analizada la información por sus respectivos equipos de sistemas verifican que la brecha de seguridad ha afectado a datos personales de 1.515.000 y 92.550 clientes, respectivamente.

Asimismo, resuelven notificar la brecha de seguridad a los afectados. La notificación a los afectados se llevó a cabo, entre los días 31 de marzo y 1 de abril de 2022, a los clientes de los que se disponía de la dirección de correo electrónico, mediante el envío masivo de comunicaciones electrónicas; y por correo postal a los restantes los días 4 y 5 de abril de 2022.

- Las tres empresas aportan el modelo de comunicación enviada a los afectados y se comprueba que se ajusta a lo especificado en el artículo 34 del RGPD.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

IBERDROLA manifiesta que al margen del incidente de seguridad objeto del presente procedimiento no se ha producido ningún otro de naturaleza análoga al mismo.

NOVENO: La entidad I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U. es una gran empresa constituida en el año 2000, y con un volumen de negocios, según AXESOR de ******CANTIDAD.1*** euros en el año 2021 y de ******CANTIDAD.2*** euros en el año 2022.

DÉCIMO: Con fecha 5 de mayo de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a I-DE, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD.

El citado Acuerdo de Inicio fue notificado conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP).

DÉCIMO PRIMERO: Con fecha 24 de mayo de 2023, I-DE presenta escrito por el que solicita la acumulación del presente expediente con el EXP202305587, así como la suspensión del plazo para la emisión de las alegaciones en tanto no se resuelva acerca de esta petición, indicando lo siguiente:

Entiende I-DE que los hechos que sirven de base al ejercicio de la potestad sancionadora que trata de ejercer la Agencia son o tienen una base única que afecta a los dos expedientes sancionadores que han sido aperturados como diferenciados, por lo que solicita la acumulación de ambos procedimientos sancionadores al entender que existe una conectividad necesaria entre los mismos, esto es, que se trata una misma situación que puede redundar en la responsabilidad de ambos. Entiende por ello I-DE que los términos de dicha responsabilidad, total, parcial, en grado de autor, de colaborador o cualquiera otro que proceda de las referencias penales solo pueden apreciarse si se analiza el procedimiento en su conjunto.

Sostiene I-DE que la falta de acumulación en el presente caso podría implicar una doble imputación a dos entidades de unos mismos hechos, que a mayor abundamiento pertenecen al mismo grupo empresarial, en concreto al grupo Iberdrola de los que IBERDROLA es la sociedad matriz.

De no acumularse ambos expedientes, manifiesta I-DE que se impediría dilucidar cuál es el grado de responsabilidad de cada una de ellas, por cuanto los hechos se analizarían de forma separada y sin entrar a valorar la supuesta actuación simultánea, en términos de responsabilidad, de las dos entidades contra lo que ambos procedimientos se dirigen. De esta forma, podría estarse produciendo una doble imputación de los mismos hechos a ambas entidades sin valorar si la misma es o no compartida o si el reproche sancionador dirigido separadamente contra ambas no debería ser objeto de reducción como consecuencia de esa supuesta concurrencia de responsabilidad. Con ello, se limita, en los términos establecidos en la jurisprudencia constitucional que a continuación se reproduce, el derecho a la defensa de I-DE, al no poder analizar las circunstancias concurrentes en el caso de una forma unificada como consecuencia de la fragmentación provocada por la apertura de dos procedimientos diferenciados.

Entiende I-DE que concurren los presupuestos establecidos en el artículo 57 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) que justifican la acumulación de los procedimientos, así como la individualización de la pertinencia de su aplicación al presente supuesto:

A) Existencia de "íntima conexión" o "identidad sustancial".

Señala I-DE que, en el caso presente, el día 18 de marzo de 2022 se produjo una brecha de seguridad de los datos personales, notificada inicialmente por I-DE. Es esta misma brecha de seguridad la que determina la apertura del presente procedimiento

en el que se atribuye responsabilidad a i-DE, así como el de aquel que se pretende acumular con el presente, abierto para dilucidar la responsabilidad de IBERDROLA.

Indica I-DE que la conectividad, en el presente supuesto, deriva, por tanto, de que se trata de depurar responsabilidad a dos personas jurídicas, pero por un mismo hecho: es la propia Agencia la que deja claro que se trata de una única brecha de seguridad y que sobre la misma es sobre la que se van a fundar, en su caso, las responsabilidades subjetivas de I-DE, en el presente procedimiento, y de IBERDROLA en el procedimiento cuya acumulación se solicita.

Por tanto, concluye I-DE que, existiendo unos únicos hechos por los que se imputa responsabilidad tanto a i-DE como a IBERDROLA, resulta evidente que es necesaria la valoración conjunta de los mismos para poder determinar si existe una responsabilidad conjunta o separada de ambas entidades, así como si la responsabilidad lo sería por distinto título en uno y otro caso.

B) Que le corresponda al mismo órgano la tramitación y resolución del procedimiento.

Señala I-DE que, junto con el anterior requisito, la LPACAP impone el respeto al principio general de competencia del órgano que ha de dictar la resolución, requisito que se cumple en el presente supuesto, dado que la Ley atribuye la competencia para la tramitación de ambos procedimientos a un único órgano sancionador, por lo que con la acumulación no se pierde ni se difumina esa competencia como consecuencia de la existencia potencial de órganos de instrucción diferente.

A juicio de I-DE, el efecto esencial de la acumulación de expedientes es el de que todas las cuestiones a resolver deben ser examinadas en un solo procedimiento y decididas en un único acto final que valore conjuntamente las responsabilidades de todos los implicados.

Señala I-DE que el esquema que acaba de analizar tiene, sin duda, características especiales en el ámbito sancionador por la propia estructura y el juicio de valor que la misma encierra.

Trae a colación varias Sentencias del Tribunal Constitucional para reseñar que los principales principios y garantías constitucionales del orden penal y del proceso penal han de observarse, con ciertos matices, en el procedimiento administrativo sancionador como el derecho a ser informado de la acusación (SSTC 31/1986, 190/1987, 29/1989) y a utilizar los medios de prueba pertinentes para la defensa (SSTC 2/1987, 190/1987 y 212/1990), así como el derecho a la presunción de inocencia (SSTC 13/1982, 36 y 37/1985, 42/1989, 76/1990 y 138/1990), derechos fundamentales todos ellos que han sido incorporados por el legislador a la normativa reguladora del procedimiento administrativo común.

Entiende I-DE que la fragmentación del procedimiento en dos procedimientos separados afecta sustancialmente a la determinación y constatación de los hechos relevantes en el mismo, así como a la delimitación de las potenciales responsabilidades que pudieran corresponder a las entidades a las que se dirigen los procedimientos cuya acumulación se solicita.

Concluye por ello I-DE que la acumulación es una exigencia de la adecuada instrucción y de la garantía del derecho de defensa y que la tramitación por separado de dos expedientes sancionadores a dos personas jurídicas distintas por los mismos hechos es perjudicial para sus intereses.

Entiende I-DE que la falta de acumulación en el presente caso podría implicar una doble imputación a I-DE e IBERDROLA, como se ha dicho, de unos mismos hechos, sin que la acumulación permita dilucidar cuál sería el grado de responsabilidad de cada una de ellas, por cuanto los hechos se analizarían de forma separada y sin entrar a valorar la supuesta actuación simultánea, en términos de responsabilidad, de las dos entidades contra lo que ambos procedimientos se dirigen.

Entiende que mantener la separación de los procedimientos supone en términos procesales un fraccionamiento de la causa que condiciona la actuación instructora y de propuesta porque aparecen instrucciones diferentes, valoraciones y pruebas potencialmente diferentes y, por tanto, criterios que pueden ser, igualmente, diferenciados.

Por todo lo expuesto, I-DE solicita la acumulación de los dos expedientes citados y que se tenga también por solicitada expresamente la suspensión del plazo para la formalización de alegaciones hasta que se resuelva el incidente de acumulación que se plantea conforme al presente escrito.

Asimismo, entiende I-DE que, teniendo en cuenta la naturaleza de lo solicitado y la incidencia en la instrucción de los expedientes en cuestión y, finalmente, en el derecho de defensa de los interesados en ambos procedimientos, al afectar sustancialmente al contenido de las alegaciones que I-DE podría efectuar en el supuesto de acordarse la mencionada acumulación, con la consiguiente merma de su derecho a la tutela judicial efectiva en su modalidad de servirse de los medios de prueba necesarios para la adecuada defensa de sus derechos, solicitamos expresamente la suspensión del plazo para la formalización de las alegaciones de forma que las mismas puedan realizarse conforme al criterio de instrucción que estamos solicitando.

Por ello, solicita I-DE la suspensión del plazo para la formalización de alegaciones hasta que se resuelva el incidente de acumulación que se plantea conforme al presente escrito.

DÉCIMO SEGUNDO: Con fecha 30 de mayo de 2023 I-DE presentó escrito de alegaciones al Acuerdo de Inicio.

DÉCIMO TERCERO: Con fecha 2 de enero de 2024 se formuló Propuesta de Resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancionara a I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U. con NIF A95075578, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, con multa administrativa de 2.500.000 euros (dos millones y medio de euros) y por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD, con una multa de 1.000.000 euros (un millón de euros).

DÉCIMO CUARTO: Con fecha 22 de enero de 2024, se recibe en esta Agencia, en tiempo y forma, escrito de I-DE en el que aduce alegaciones a la propuesta de resolución.

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

HECHOS PROBADOS

PRIMERO: Primera notificación de brecha de datos personales

Con fecha 18 de marzo de 2022, I-DE notifica a la AEPD una brecha de datos personales en la que informa de lo siguiente:

(...)

Se indica que el número de afectados es de 4,5 millones de clientes de esta sociedad.

Indica como fecha de inicio de la brecha el 9 de marzo de 2022

Indica como fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto afectados datos personales: 17 de marzo de 2022.

SEGUNDO: Segunda notificación de brecha de datos personales

Con fecha 29 de marzo de 2022 I-DE presenta una nueva notificación ampliando la información sobre la brecha de datos personales notificada, a través de la aportación de del informe "*Incidente ciber GEA. Descripción incidente y acciones*." fechado el 28 de marzo 2022, según el cual:

"I-DE, dentro de la prestación de servicios a sus clientes, ofrece un aplicativo web llamado Gestión de Expedientes y Acometidas (GEA): ******URL.1***

Este servicio permite a los clientes o sus representantes (instaladores) realizar los trámites pertinentes para el proceso de una conexión a la red. En el transcurso de las sesiones de la aplicación, hay un intercambio de información de datos del cliente que está sometido a los filtros de seguridad propios de la aplicación, de forma que cada cliente (o representante delegado) sólo podrá acceder a la información que corresponda a la seguridad y perfiles de acceso previsto.

Indica que el número de afectados clientes de esta sociedad es de 1.350.000

Indica como fecha de inicio de la brecha el 7 de marzo de 2022

TERCERO: Cronología del ataque

Según indica I-D, en el informe "*Incidente ciber GEA. Descripción incidente y acciones*." fechado el 28 de marzo 2022" y aportado junto con la segunda notificación de brecha de datos personales, así como en el escrito de respuesta al requerimiento de información realizado por esta AEPD, durante las actuaciones previas de investigación, presentado en fecha 1 de agosto de 2022 (Número de registro: REGAGE22e00033475096) la cronología del ataque es la siguiente:

- *"El 15 de marzo, por la tarde, se detecta un ataque contra la web de gestión de acometidas de I-DE, (GEA)*
    - ***(…)***
- *El 16 de marzo de 2022, por la mañana, se produce una ralentización general del acceso a varias webs del grupo Iberdrola.*
    - ***(…)***
- *A partir del día 17 de marzo:*
    - ***(…)***
    - *A partir del día 17 no se observa tráfico sospechoso ni afectación en ninguno de los sistemas de servicios en internet del grupo Iberdrola.*
    - *Del análisis del registro de actividad de la aplicación GEA de los últimos días se concluye con fecha 17 de marzo que se ha producido una exfiltración, entre los días 7 y 15 de marzo de 2022, de aproximadamente 4,5 millones de interesados (personas físicas).*
    - ***(…)***
    - *En fecha 28 de marzo de 2022, la Dirección de Sistemas comunica a IBERCLI y CURENERGIA la existencia de un incidente de seguridad en los sistemas de I-DE que ha podido afectar a la información referida a los clientes de estas compañías y les incluye información referida a los códigos internos de cliente de los afectados, a fin de que las compañías verifiquen si han podido verse comprometidos datos correspondientes a sus clientes. Analizada la información por IBERCLI y CURENERGIA verifican que la brecha de seguridad ha afectado a datos personales de clientes de dichas sociedades.*
    - ***(…)***

CUARTO: Sobre la aplicación GEA

Respecto al aplicativo GEA, I-DE manifiesta:

En el informe "*Incidente ciber GEA. Descripción incidente y acciones*." fechado el 28 de marzo 2022:

-"*I-DE, dentro de la prestación de servicios a sus clientes, ofrece una aplicativo web llamado Gestión de Expedientes y Acometidas (GEA):* ******URL.1***

Este servicio permite a los clientes o sus representantes (instaladores) realizar los trámites pertinentes para el proceso de una conexión a la red. En el transcurso de las sesiones de la aplicación, hay un intercambio de información de datos del cliente que está sometido a los filtros de seguridad propios de la aplicación, de forma que cada cliente (o representante delegado) sólo podrá acceder a la información que corresponda a la seguridad y perfiles de acceso previsto"

-I-DE dispone de un sistema (SIC) del que GEA es un servicio web, propio y exclusivo para el tratamiento de sus procesos y datos de clientes, siendo los equipos de negocio y sistemas encargados del desarrollo, evolución y mantenimiento de este sistema, igualmente, exclusivos para I-DE.

-En el "*Manual de Acceso clientes titulares, GEA*", aportado por I-DE se describe la metodología para dar de alta de un usuario (Documento nº6 de la entrada REGAGE23e00004673128), en el que se indica que para el desarrollo del proceso de alta de un nuevo usuario es preciso disponer de una dirección de correo electrónico valida y accesible, a la que se envía de forma automática un enlace, individualizado para cada usuario, que permite establecer la contraseña para el primer acceso, validando de esta forma el alta en la aplicación.

-En el escrito de respuesta de requerimiento realizado por esta AEPD, presentado con fecha 21 de febrero de 2023 (Número de registro: REGAGE23e00011000318) indica I-DE que:

(…)

Esta URL se mostraba a los usuarios validados en el momento del incidente.

IBERDROLA S.A., que le presta diferentes servicios a I-DE y a otras empresas del Grupo, entre ellos, de "Soporte y mantenimiento de infraestructura IT" y de "Desarrollo de aplicaciones", actuando en consecuencia, como encargada del tratamiento de I-D, en su escrito de respuesta al requerimiento de información realizado por esta AEPD durante el período de investigaciones previas, presentado en fecha 24 de enero de 2023 (Número de registro: REGAGE23e00004670187), a solicitud de información relativa a la descripción del control y permisos de acceso a la aplicación de cada uno de los perfiles identificados, IBERDROLA responde:

(…)

QUINTO: Causas que hicieron posible la brecha

En el "*Resumen Informe Forense Incidente Seguridad GEA*", de fecha 23 de marzo de 2022, aportado por I-DE junto a su escrito de respuesta de requerimiento realizado por esta AEPD, presentado con fecha 1 de agosto de 2022 (Número de registro: REGAGE22e00033475841), se indica:

(…)

-I-DE indica lo siguiente:

(…)

-IBERDROLA S.A., que le presta diferentes servicios a I-DE y a otras empresas del Grupo, entre ellos, de “Soporte y mantenimiento de infraestructura IT” y de “Desarrollo de aplicaciones”, actuando en consecuencia, como encargada del tratamiento de I-D, en su escrito de respuesta al requerimiento de información realizado por esta AEPD durante el período de investigaciones previas, presentado en fecha 24 de enero de 2023(Número de registro: REGAGE23e00004670187), indica lo siguiente:

(…)

SEXTO: Medidas recomendadas

Consta en el documento “Resumen Informe Forense Incidente Seguridad GEA”, de 23/03/2022, aportado por I-DE en su escrito de 1/08/2022, las siguientes recomendaciones:

(…)

SÉPTIMO: medidas inmediatas tras la brecha

I-DE, en su escrito de respuesta de requerimiento realizado por esta AEPD, presentado con fecha 21 de febrero de 2023 (Número de registro: REGAGE23e00011000318) indica:

(…)

IBERDROLA, S.A., en su escrito de respuesta al requerimiento de información realizado por esta AEPD durante el período de investigaciones previas, presentado en fecha 24 de enero de 2023 (Número de registro: REGAGE23e00004670187), adjunta como “Documento nº 11”, el “Plan Urgente de Ciberseguridad”. En el mismo se indica, entre otras, las siguientes medidas: Seguridad de Aplicaciones:

(…)

OCTAVO: medidas de seguridad implantadas con anterioridad al incidente

Entre otras, se aportó:

(…)

NOVENO: Análisis de riesgos del tratamiento afectado por la brecha de datos personales

A solicitud de esta AEPD de copia del análisis de riesgos sobre los derechos y libertades de las personas físicas realizado sobre la actividad del tratamiento que ha sufrido la brecha de seguridad con anterioridad a la incidencia, I-DE aportó el esquema seguido en el seno del Grupo Iberdrola para la valoración del riesgo en el tratamiento de los datos personales se lleva a cabo conforme al mismo.

Aporta dicho esquema que se detallan ciertas amenazas o circunstancias como "colectivos vulnerables" "acceso a los datos personales por más de 10 personas" "transferencias internacionales" "tratamientos a gran escala" "perfiles con efectos jurídicos". Estas circunstancias se establecen como preguntas y, según se responda "si" o "no", se le aplica un resultado.

Asimismo, indica que "*Se adjuntan, como Documento Nº 8 documento explicativo de la lógica seguida para el cálculo del nivel de riesgo conforme a esta metodología. Dicha metodología se encuentra implantada de forma automatizada en la propia herramienta corporativa de registro de actividades de tratamiento, de forma que en el propio proceso de registro determina el nivel de riesgo del tratamiento. Así pues, la aplicación de dicha metodología en relación con el tratamiento ***TRATAMIENTO.1 arrojó como resultado un nivel de riesgo MEDIO, como se recoge en el Documento Nº 7 arriba referido*.

En dicho documento 8 se analizan circunstancias o amenazas en el sentido del esquema indicado, las cuales se trasladan al Registro de Actividades de Tratamiento.

DÉCIMO: Número de personas afectadas y tipo de datos afectados

1.350.000 de clientes de I-DE afectados.

Tipo de datos afectados:

Nombre y apellidos
Dirección de correo electrónico
Número de Fax
Teléfono
Dirección postal
NIF/DNI
Código cliente
Código sociedad

DÉCIMO PRIMERO: Comunicación a los afectados

En el escrito de respuesta al requerimiento de información realizado por esta AEPD, durante las actuaciones previas de investigación, presentado en fecha 1 de agosto de 2022 (Número de registro: REGAGE22e00033475096), I-DE manifiesta que ha comunicado a los afectados la brecha de datos personales, indicando:

> "*Las citadas comunicaciones fueron remitidas a los clientes de i-DE de los que se disponía de dirección de correo electrónico a través de este medio mediante la realización de varios envíos entre los días 31 de marzo y 12 de abril de*

2022, notificándose la brecha por correo ordinario a los restantes cliente entre los días 30 de marzo y 7 de abril de 2022."

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II
Cuestiones previas

I-DE es una gran empresa del Grupo Iberdrola dedicada a la distribución de energía eléctrica y para ello realiza tratamientos de datos personales como responsable de un número muy elevado de personas pues, según manifiesta, trata datos de 21 millones de clientes.

Por tanto, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que I-DE realiza, entre otros tratamientos, la recogida, conservación, consulta, utilización, supresión, etc., de datos personales de personas físicas, tales como: nombre, apellidos, DNI, dirección postal, número de teléfono, dirección de correo electrónico, datos bancarios, datos relativos al suministro y al consumo eléctrico, cuenta corriente, etc.

Asimismo, IBERDROLA S.A. le presta diferentes servicios a I-DE y a otras empresas del Grupo, entre ellos, de “Soporte y mantenimiento de infraestructura IT” y de “Desarrollo de aplicaciones”, actuando en consecuencia, como encargada del tratamiento de I-D.

En el caso que nos ocupa, la brecha de seguridad sufrida ha afectado a datos personales tratados por I-DE en su condición de responsable del tratamiento, al determinar los fines y medios respecto de esos tratamientos, en virtud del artículo 4.7 del RGPD.

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

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse producido un acceso indebido por un tercero no autorizado a datos personales tratados por I-DE.

III

Sobre la solicitud de acumulación y la suspensión del plazo para formular alegaciones

Respecto de la solicitud de acumulación del presente expediente y el EXP202305587 realizada por I-DE, procede señalar que el artículo 57 de la LPACAP establece:

> *"El órgano administrativo que inicie o tramite un procedimiento, cualquiera que haya sido la forma de su iniciación, podrá disponer, de oficio o a instancia de parte, su acumulación a otros con los que guarde identidad sustancial o íntima conexión, siempre que sea el mismo órgano quien deba tramitar y resolver el procedimiento.*
> *Contra el acuerdo de acumulación no procederá recurso alguno".*
> (el subrayado es nuestro)

Por tanto, es una posibilidad que tiene la Administración, no estando obligada a proceder a la acumulación en caso de ser solicitada. Si embargo, ello no obsta para que se motive a continuación las razonas por las cuales se ha considerado oportuno tramitar ambos procedimientos sancionadores por separado.

Así, si bien los dos expedientes sancionadores, uno dirigido contra I-DE y otro contra IBERDROLA, S.A., parten del mismo incidente de seguridad (el ataque a la aplicación GEA), el mismo ha producido dos brechas de datos personales diferentes y diferenciadas, tal y como se refleja en los Antecedentes de Hecho de la presente propuesta, especialmente en el Antecedente de hecho Octavo, donde se reseña la información recabada durante la fase de actuaciones previas de investigación llevadas a cabo por esta AEPD.

Así, por un lado, el ataque se inició a través de un aplicativo web de I-DE, aprovechando una vulnerabilidad del mismo y que permitió el acceso a la base de datos de I-DE y que afectó a la confidencialidad de 1.350.000 clientes de I-DE. Por

tanto, el presente procedimiento sancionador se dirige exclusivamente a I-DE como responsable del tratamiento de los datos personales de sus clientes y como consecuencia de una vulnerabilidad existente en un aplicativo web suyo.

De otro lado, en el ciberataque no sólo se vieron afectados datos personales de I-DE, sino que, al acceder a la base de datos de I-DE, la cual se encontraba alojada en un sistema en el que coexisten bases de datos de otras empresas del mismo grupo, sino que también se consiguió superar la separación lógica y acceder a las bases de datos de otras dos empresas, IBERCLI y CURENERGÍA, afectando a la confidencialidad de datos personales de clientes de estas dos últimas. Estas diferentes bases de datos de diferentes empresas se alojan o se llevan a cabo en un sistema mantenido y soportado por la empresa IBERDROLA, S.A., la cual, en consecuencia, es encargada de tratamiento de todas ellas, es decir, de I-DE, IBERCLI y CURENERGÍA.

Este hecho ha supuesto que se inicie un procedimiento sancionador a IBERDROLA, S.A., pero por su responsabilidad como encargada de tratamiento de IBERCLI y de CURENERGÍA y exclusivamente por la brecha de datos personales que ha afectado únicamente a los datos personales de los clientes de estas dos empresas comercializadoras y solamente atendiendo a la responsabilidad que puede tener IBERDROLA, S.A. en cuanto a la configuración de las bases de datos que gestiona respecto de estas dos empresas afectadas.

En este sentido, esa afectación a datos personales de clientes alojados en bases de datos ajenas a I-DE no puede formar parte de este procedimiento sancionador dirigido exclusivamente a examinar la conducta de I-DE, por cuanto no es responsable ni de los datos personales de clientes afectados que pertenecen a otras empresas, ni de la posible falta de adopción de las medidas adecuadas para su protección o para la separación absoluta entre unas y otras. Por tanto, se ha de analizar de forma independiente la gestión de las bases de datos que realiza IBERDROLA, S.A. respecto de esas terceras empresas, sin que pueda responder I-DE por posibles incumplimientos de la normativa de protección de datos en que hayan podido incurrir esas terceras empresas.

Así lo manifestó I-DE en su escrito de respuesta de requerimiento realizado por esta AEPD, presentado con fecha 1 de agosto de 2022, en el que al solicitársele información sobre los datos afectados por la brecha relativos a clientes de IBERCLI y CURENERGÍA, respondió que "*I-DE no tiene acceso a los datos de las personas que han podido verse afectadas por la brecha de seguridad y que no tengan la condición de clientes de la citada entidad al no encontrarse su punto de suministro asignado a la red gestionada por i-DE. Ello significa que i-DE no tiene capacidad para conocer ningún tipo de información relacionada con quienes siendo clientes de IBERCLI o de CURNERGIA no lo sean de esta distribuidora*"

Por tanto, estando dirigido los procedimientos sancionadores a diferentes sujetos (dos empresas diferentes), estar afectados los datos personales de clientes de diferentes empresas, no teniendo I-DE nada que ver con los datos de clientes ajenos, tramitarse por vulnerabilidades o incumplimientos respecto de sistemas diferentes (uno un aplicativo web, otra una base de datos), etc., es por lo que no se ha considerado por esta AEPD acumular los dos expedientes, sino tramitar los dos procedimientos sancionadores de forma separada, al estar claramente separada la responsabilidad

que se atribuye a cada uno, así como tratarse de brechas de datos personales diferentes y que afectan a datos personales tratados por responsables diferentes.

Asimismo, ello no le produce indefensión a I-DE por cuanto en todo momento conoce los hechos que se le imputan, la infracción que los mismos suponen, su tipificación, la responsabilidad en que ha incurrido, así como que ha tenido y tiene la oportunidad de formular alegaciones y presentar cuanta documentación considere oportuna en defensa de sus intereses que le permite la legislación aplicable.

Por último, en cuanto a la solicitud de suspensión del plazo para formular alegaciones al Acuerdo de Inicio mientras no se decida sobre la acumulación de los dos procedimientos, se significa que dicha posibilidad no existe ni en la normativa aplicable de protección de datos (RGPD Y LOPDGDD) ni en la LPACAP. Por el contrario, en esta última ley lo que se establece es la obligatoriedad de que los trámites que deban ser cumplimentados por los interesados son de obligado cumplimiento:

> *"Artículo 73. Cumplimiento de trámites.*
> *1. Los trámites que deban ser cumplimentados por los interesados deberán realizarse en el plazo de diez días a partir del siguiente al de la notificación del correspondiente acto, salvo en el caso de que en la norma correspondiente se fije plazo distinto*."

Por tanto, no procede la solicitud de suspensión, al no existir legalmente esta posibilidad, ni la misma ha tenido efecto alguno, no habiéndose suspendido, en consecuencia, el plazo para formular alegaciones.

IV

Respuesta a las alegaciones al Acuerdo de Inicio

En respuesta a las alegaciones presentadas por I-DE se debe señalar lo siguiente:

PRIMERA: SOBRE LA ACUMULACIÓN DE LOS PROCEDIMIENTOS

Reitera I-DE de nuevo la solicitud de acumulación y se remite a la solicitud presentada al efecto el 24 de mayo de 2023.

A este respecto, procede remitirse a lo argumentado en el Fundamento de Derecho anterior, en el que se da debida respuesta a esta cuestión.

SEGUNDA. – SOBRE LAS ESPECIALES CIRCUNSTANCIAS ACAECIDAS EN RELACIÓN CON LA TRAMITACIÓN DEL PRESENTE EXPEDIENTE Y LA VULNERACIÓN DE LOS PRINCIPIOS DE BUENA FE, CONFIANZA LEGÍTIMA Y SEGURIDAD JURÍDICA

Alega I-DE que esta AEPD ha vulnerado los principios de seguridad jurídica, buena fe y confianza legítima establecidos en el artículo 3.2 e) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJSP) ya que mediante escrito fechado el 18 de abril de 2022, de la División de Innovación Tecnológica de la AEPD, se indica, en relación con la información adicional aportada por I-DE relativa a la brecha de datos personales sufrida por ella, que "*Tras el análisis de la información*

adicional aportada, la brecha de seguridad ha sido actualizada en el registro de notificaciones de brechas de seguridad y no se prevé el inicio de otras acciones por parte de esta Agencia", pero que sin embargo, posteriormente y sin que conste ninguna actuación posterior hasta la fecha del primer requerimiento de información que se le dirige (escrito firmado el 8 de julio de 2022 por el Inspector actuante) de lo que parece desprenderse la iniciación por la AEPD de actuaciones de investigación, sin existir acuerdo o decisión alguna en este sentido.

Entiende I-DE que ello pone de manifiesto que no procedía la realización de investigación adicional relacionada con la brecha por cuanto la AEPD al firmar el referido escrito de 18 de abril consideró adecuadas las manifestaciones efectuadas por I-DE, no apreciando en la brecha la concurrencia de elemento alguno que justificase la realización de actuaciones de investigación tendentes a determinar si se había producido una presunta vulneración de la normativa de protección de datos.

Sin embargo, continua I-DE, la AEPD el 9 de mayo de 2022, acuerda la admisión a trámite de reclamaciones (formuladas con anterioridad al 18 de abril de 2022) y la iniciación de actuaciones previas de investigación, pero sin que conste en el expediente ninguna actuación o circunstancia relacionada con este caso que hubiera sido aportada o acaecido en el período que mediaba entre el 18 de abril y la fecha de admisión a trámite y que justifique el inicio de las mismas.

Asimismo, entiende I-DE que el escrito de 18 de mayo de 2022 supone que la AEPD consideraba que la información recibida de ella sobre la brecha era suficiente para entender que no concurría en ella responsabilidad alguna por un supuesto incumplimiento de la normativa de protección de datos, lo que determinaba el archivo de un expediente que, sin embargo, la AEPD decide abrir días después sin que concurra indicio alguno que implique un cambio sustancial en la naturaleza, circunstancias o severidad de la brecha. De ello concluye I-DE que la AEPD adoptó una decisión que contradice frontalmente con la previa adoptada apenas 20 días antes.

Frente a ello, procede señalar que en modo alguno puede aceptarse la interpretación de I-DE del escrito que recibió el 18 de mayo de 2022. Así, dicho escrito está firmado de forma genérica por la AEPD, proviene de la División de Innovación Tecnológica, la cual se encarga de recibir las brechas de seguridad y registrarlas en el registro al efecto, y en el cual se indicó lo siguiente:

> *"En relación con la información adicional aportada mediante registro de entrada REGAGE22e00010072289, relativa a una brecha de datos personales en un tratamiento de I-DE REDES ELECTRICAS INTELIGENTES S.A.U. informamos que:*
>
> *Tras el análisis de la información adicional aportada, la brecha de seguridad ha sido actualizada en el registro de notificaciones de brechas de seguridad y no se prevé el inicio de otras acciones por parte de esta Agencia.*
>
> *No obstante, le recordamos la necesidad de investigar las causas del incidente hasta entender cómo y por qué ha sucedido, y la obligación de tomar las acciones oportunas para evitar que vuelva a suceder y minimizar el impacto*

potencial sobre los afectados, así como la obligación de documentar cualquier incidente de seguridad que pueda afectar a los datos personales como los hechos relacionados con los mismos y las medidas correctivas aportadas tal y como establece el artículo 33.5 del RGPD.

Si en el trascurso del tiempo obtuviera indicios que impliquen un cambio sustancial en la naturaleza, circunstancias o severidad de la brecha, puede realizar una nueva notificación completa a través de nuestra sede electrónica https://sedeagpd.gob.es/sede-electronica-web/.

Así mismo, le informamos que en el siguiente enlace tiene a su disposición la guía para la gestión y notificación de brechas de seguridad de los datos personales publicada por esta Agencia: https://www.aepd.es/media/guias/1ome-brechas-seguridad.pdf"

Como encabezado consta "DIVISIÓN DE INNOVACIÓN TECNOLÓGICA"

En el lateral izquierdo del escrito se indica que "Firmado electrónicamente por: Agencia Española de Protección de Datos. A fecha 18/04/2022"

No aparece firmado por la Directora de la Agencia, no tiene parte dispositiva en la que se acuerde o resuelva algo, ni tiene indicación de recurso alguno contra la misma.

Por tanto, y en contra de lo que afirma I-DE, este escrito no tiene carácter decisorio, ni por su contenido, que únicamente contiene una previsión y que en modo alguno puede entenderse que supone que esta AEPD ha valorado y decidido que no concurría en I-DE responsabilidad alguna por un supuesto incumplimiento de la normativa de protección de datos, lo que supondría el archivo de unas actuaciones -tal y como ha querido entender I-DE-, ni tampoco por su forma, pues ni siquiera formalmente refleja una decisión, ni mucho menos una resolución de archivo de actuación alguna, pues para que ello sea así, el único órgano competente para ello es la actual Directora de la AEPD. Así, el Artículo 13 del Estatuto de la AEPD, aprobado mediante Real Decreto 389/2021, de 1 de junio, se determinan las funciones de la Presidencia:

1. *Corresponde a la Presidencia de la Agencia Española de Protección de Datos:*

   d) Dictar las resoluciones y directrices que requiera el ejercicio de las funciones de la Agencia, en particular las derivadas del ejercicio de las competencias previstas en el artículo 57 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y del ejercicio de los poderes de investigación y de los poderes correctivos dispuestos en el artículo 58 del citado Reglamento.

Por tanto, para proceder al archivo de unas actuaciones investigación se requiere, primero, que se hayan iniciado (bien por haberse admitido a trámite una reclamación, bien por iniciativa propia, lo cual en ambos casos exige una resolución expresa firmada por la Directora), lo cual no había sucedido en el momento de emitirse el referido escrito de la División de Innovación Tecnológica y, en segundo lugar, es necesario de nuevo una resolución expresa por parte de la Directora archivando

dichas actuaciones por entender, ahora sí, que de la información recabada en dichas investigaciones, no se concluye la existencia de infracción en la normativa de protección de datos, lo cual no se había producido.

En el presente caso, tras la notificación de la brecha de datos personales por parte de I-DE, se presentaron varias reclamaciones por personas afectadas por la misma, las cuales fueron admitidas a trámite de forma conjunta por la AEPD en cumplimiento del artículo 64 LOPDGDD:

Artículo 64. Forma de iniciación del procedimiento y duración.

> *1.Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.*
> *En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.*
>
> *2.Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.*
>
> *Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.*
>
> *Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica.*
>
> *Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.*
>
> *Artículo 67. Actuaciones previas de investigación.*
>
> *1.Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.*

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2.Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica. (el subrayado es nuestro)

De dicha normativa no se infiere en modo alguno que la AEPD tenga que justificar de la manera que exige I-DE el inicio de actuaciones previas en el sentido de que tenga que haber algo nuevo o alguna circunstancia nueva o de que las reclamaciones hayan tenido que aportar circunstancias nuevas y diferentes respecto de la documentación aportada por I-DE en su notificación de la brecha a esta Agencia, pues ello no viene exigido por la normativa indicada, además de que no se puede pretender que los afectados aporten algo nuevo, al margen de conocer que se ha vulnerado la confidencialidad de sus datos personales por un ciberataque de cuyas circunstancias desconocen.

Precisamente las actuaciones previas de investigación se realizan para esclarecer los hechos y las circunstancias de lo acontecido, recabando más información al objeto de poder determinar o no la existencia de una posible infracción de la normativa en materia de protección de datos. En este sentido, el inicio de investigaciones previas y su realización, potestad de la AEPD con o sin reclamaciones, no prejuzga nada, sino que permite recabar la información necesaria para determinar si hay indicios o no de infracción. Incluso tras dicha investigación, puede ser que se archiven las actuaciones por entender, a la vista de la información recabada, que no existen indicios de infracción. Lo cual, en el presente caso, no ha sucedido.

Lo que sí indica la normativa es que, tras la presentación de reclamaciones, esta Agencia debe decidir si las admite a trámite o no, habiendo decidido finalmente su admisión mediante, esta vez sí, Acuerdo de admisión a trámite, firmado por la Directora de la Agencia con fecha 9 de mayo de 2022. Y, como indica el artículo 67.2 LOPDGDD referenciado, la AEPD puede llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias. Es una potestad que tiene atribuida por el RGPD y por la LOPDGDD.

Asimismo, y a mayor abundamiento de todo, incluso en el supuesto de no haber existido las reclamaciones, el escrito de la División de Innovación Tecnológica no hubiera sido tampoco óbice ni obstáculo para el ejercicio de las potestades de investigación que tiene la AEPD de conformidad con el citado artículo 64.2 que determina que "*Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación…*"

Por tanto, el presente procedimiento sancionador no se ha iniciado por el contenido o por alguna información nueva aportada en las reclamaciones, sino por la información y documentación obtenida tras el período de actuaciones previas de investigación, al inferirse de la misma posibles vulneraciones a la normativa en materia de protección de datos.

Por último, trae a colación I-DE la Sentencia del Tribunal Supremo, de 22 de febrero de 2016 (recurso 4048/2013), entendiendo que es plenamente aplicable al caso, en la que se indica:

> *"Acorde con los hechos sucintamente expuestos podemos considerar lesionada la confianza legítima, pues la Administración no puede adoptar decisiones que contravengan las perspectivas y esperanzas fundadas en las propias decisiones anteriores de la Administración. Cuando se confía en la estabilidad de su criterio, evidenciado en múltiples actos anteriores en un mismo sentido, que lleva al administrado a adoptar determinadas decisiones, se genera una confianza basada en la coherencia del comportamiento administrativo, que no puede defraudarse mediante una actuación sorprendente. […]*
> *Conviene tener en cuenta que confianza legítima requiere, en definitiva, de la concurrencia de tres requisitos esenciales. A saber, que se base en signos innegables y externos (1); que las esperanzas generadas en el administrado han de ser legítimas (2); y que la conducta final de la Administración resulte contradictoria con los actos anteriores, sea sorprendente e incoherente (3). Exactamente lo que acontece en el caso examinado, a tenor de los hechos antes relatados.*
> *Recordemos que, respecto de la confianza legítima, venimos declarando de modo reiterado, por todas, Sentencia de 22 de diciembre de 2010 (recurso contencioso-administrativo núm. 257 / 2009), que << el principio de la buena fe protege la confianza legítima que fundadamente se puede haber depositado en el comportamiento ajeno e impone el deber de coherencia en el comportamiento propio. Lo que es tanto como decir que el principio implica la exigencia de un deber de comportamiento que consiste en la necesidad de observar de cara al futuro la conducta que los actos anteriores hacían prever y aceptar las consecuencias vinculantes que se desprenden de los propios actos constituyendo un supuesto de lesión a la confianza legítima de las partes "venire contra factum propium >>*

A este respecto se significa que la doctrina establecida en la misma no es "de aplicación al presente caso, ya que, como se ha indicado anteriormente, ni ha sido una decisión de esta Administración, ni por su forma ni por su contenido, ni ha provocado que se confíe en la estabilidad de su criterio, ya que no ha habido ningún criterio decisorio al respecto, ni mucho menos evidenciado en múltiples actos anteriores en un mismo sentido, por lo que la actuación de esta Agencia en relación a lo alegado no ha supuesto una conducta final de ella que resulte contradictoria con actos anteriores que sea sorprendente ni incoherente, en el sentido de la doctrina del Tribunal.

Por lo expuesto, se desestima la alegación formulada.

TERCERA.- SOBRE LA AFECTACIÓN ADICIONAL A LOS PRINCIPIOS DEL DERECHO SANCIONADOR DERIVADOS DE LA INTERPRETACIÓN EFECTUADA POR LA AEPD

Alega I-DE en este apartado que el Acuerdo de Inicio incurre en importantes vulneraciones de los principios de derecho administrativo sancionador, ya que implica la imposición de dos infracciones cuyo contenido es, en realidad idéntico o respecto de las que, cuanto menos, cabe apreciar la subsunción de una de ellas en la otra:

1.Vulneración del principio non bis in ídem

Alega I-DE que en el Acuerdo de Inicio la AEPD considera que las medidas de seguridad implementadas por ella no han sido, a su juicio, las adecuadas y que ello implica una doble vulneración del RGPD, por una parte, entiende que I-DE no ha adoptado las medidas técnicas y organizativas adecuadas, exigidas por el artículo 32 del RGPD; y,
por otra, entiende vulnerado el principio de seguridad, quebrantando, supuestamente, el artículo 5.1 f) del RGPD, del que el artículo 32 no es sino mera concreción.

Entiende I-DE que ello supone que se imponen dos sanciones diferenciadas, respectivamente, por considerar que mi representada carece de las adecuadas medidas de seguridad y porque entiende que se ha producido, por carecer de tales medidas, una brecha de confidencialidad de los datos personales. Y, además, establece para ambas supuestas infracciones unas circunstancias modificativas de la responsabilidad de I-DE en todo punto idénticas, tanto en su determinación como en la fundamentación jurídica de su imposición.

Señala I-DE que de ello se desprende que la AEPD considera que un mismo hecho (la supuesta insuficiencia de medidas de seguridad) sería constitutivo de dos infracciones del mismo bien jurídico protegido (la adecuada garantía de los derechos y libertades de los interesados). Y ello, por cuanto se sancionaría, por una parte, la ausencia de las medidas de seguridad que la AEPD considera necesario adoptar y, por otra, el principio de seguridad y confidencialidad, que exige la adopción de tales medidas.

Por tanto, sostiene I-DE que, incurriendo en la triple identidad de sujeto, hecho y bien jurídico protegido, no cabe duda de que se ha vulnerado el principio de non bis in idem, por lo que cabría sólo imputar y sancionar por una sola infracción, que en este caso sería únicamente por el artículo 32, ya que sólo cabría apreciar la supuesta insuficiencia de medidas de seguridad.

Frente a ello, procede explicar la diferencia entre la vulneración del art. 5.1.f y el artículo 32 del RGPD, la cual se ampliará en el punto siguiente respecto al alegación relativa a la existencia de concurso medial, así como la diferente tipificación en apartados incluso distintos del art. 83 del RGPD y la diferente calificación de ambos a los efectos de la prescripción en la LOPDGDD.

El art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales por ausencia o deficiencia de medidas de cualquier tipo.

Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita "mediante la aplicación de medidas técnicas y organizativas apropiadas", que no son estrictamente de seguridad.

Indica I-DE que las medidas técnicas y organizativas apropiadas a las que hace mención el art. 5.1.f) RGPD 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.

Cuando el art. 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD lo hace en el sentido previsto en el art. 25 del RGPD relativo a la privacidad desde el diseño.

Este precepto determina que,

> "*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados*" (el subrayado es nuestro)

Debe señalarse que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el art. 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. De seguridad. Sólo de seguridad.

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo independientemente de que se haya producido una quiebra de seguridad, mientras que en el caso del artículo 5.1.f) del RGPD se debe garantizar la disponibilidad, confidencialidad e integridad y se materializa, en este caso, con la pérdida de la confidencialidad de los datos. Como se puede observar los dos artículos se refieren a conductas diferentes, aunque puedan estar relacionados.

Entrando ya de lleno en el examen del non bis in ídem, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que,

"(…) *Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.*
Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):

2. *La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.*

b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.

c) La identidad de fundamento o causal, implica que las medidas sancionadoras no pueden concurrir si responden a una misma naturaleza, es decir, si participan de una misma fundamentación teleológica, lo que ocurre entre las penales y las administrativas sancionadoras, pero no entre las punitivas y las meramente coercitivas."

Tomando como referencia lo anteriormente explicitado, no se ha vulnerado el principio non bis in ídem, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una brecha de datos personales, la infracción del art. 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y disponibilidad, la infracción del art. 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la brecha de datos personales. De hecho, si esas deficiencias en las medidas de seguridad que se detectaron en el aplicativo web de I-DE se hubieran detectado por la AEPD sin que se hubiera producido la pérdida de confidencialidad, únicamente cabría haberle sancionado por el art. 32 del RGPD.

Y todo ello frente a las alegaciones formuladas por I-DE que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el art. 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad a través de cualesquiera medidas. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de disponibilidad y confidencialidad y, mediante el art. 32 del RGPD la ausencia y/o deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes, añadimos, que infringen el

RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad y de disponibilidad.

Por último, respecto de la aplicación de idénticos agravantes en ambas infracciones, hemos de significar que las circunstancias previstas en el art. 83.2 del RGPD y las dispuestas en el art. 76.2 de la LOPDGDD son las únicas que se pueden aplicar por la AEPD para cualquier infracción.

Lo determinante en este caso, respecto de la prevista en el art. 83.2.b) del RGPD no es que coincidan en su uso, sino la fundamentación que se establezca para su consideración.

Dicho todo lo cual, no se considera que existe vulneración del principio de non bis in ídem, consagrado en el artículo 25 de la Constitución Española.

2.Subsidiariamente, existencia de concurso medial entre las dos conductas imputadas a I-DE

Alega I-DE que, por otra parte, el Acuerdo de Inicio identifica (y pretende sancionar) una pluralidad de infracciones que, supuestamente, habría cometido mi mandante (lo que se niega de plano) cuando, en realidad, una de ellas se encontraría subsumida y embebida en la otra, dando lugar un concurso medial en los términos previstos en el artículo 29.5 de la LRJSP.

Entiende I-DE que no puede sancionarse ambas infracciones, dado que la comisión de la supuesta infracción del artículo 32.1 del RGPD determinaría la supuesta vulneración del artículo 5.1.f) del mismo texto legal y se estaría sancionando por unos mismos hechos, pues considera que la supuesta infracción del artículo 5.1 f) traería necesaria e inseparablemente causa de la supuesta falta de implementación diligente de las medidas a las que se refiere el artículo 32.1 del RGPD.

Trae I-DE a colación determinada jurisprudencia (por todas, la Sentencia 339/2015 de 25 de septiembre de 2015 de la Audiencia Nacional -recurso 262/2014- que cita la Sentencia del Tribunal Supremo de 8 de febrero de 1999, -recurso 9/1996-): "*la aplicación del concurso medial exige una necesaria derivación de unas infracciones respecto de las demás y viceversa, por lo que es indispensable que las unas no puedan cometerse sin ejecutar las otras*". Así, debe existir "*una relación tal entre las infracciones concernidas que una de ellas derive necesariamente de la otra, de modo que no sea posible la comisión de una sin ejecutar la otra*" (por todas, la Sentencia de la Audiencia Nacional de 26 de diciembre de 2013, -recurso 416/2012). Por ello concluye I-DE que es evidente que se produce tal relación entre las dos infracciones que pretenden imputarse contra ella.

A este respecto, se significa, tal y como se ha señalado anteriormente, que el art. 32 del RGPD, aunque relacionado con el art. 5.1.f) del RGDP no circunscribe el principio en su totalidad.

Así, El artículo 5.1.f) del RGPD es uno de los principios relativos al tratamiento. Los principios relativos al tratamiento son, por un lado, el punto de partida y la cláusula de cierre del ordenamiento jurídico de protección de datos, constituyendo verdaderas

reglas informadoras del sistema con una intensa fuerza expansiva; por otro lado, al tener un alto nivel de concreción, son normas de obligado cumplimiento susceptibles de ser infringidas.

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.

Muestra de ello, no sólo es esta diferencia entre la vulneración del art. 5.1.f y el artículo 32 del RGPD, sino la diferente tipificación en apartados incluso distintos del art. 83 del RGPD y la diferente calificación de ambos a los efectos de la prescripción en la LOPDGDD.

En el supuesto examinado, tal y como consta en los hechos probados, hay una clara pérdida de confidencialidad puesto de manifiesto a través de un claro resultado: se produjo un acceso ilegítimo por un tercero no autorizado a datos personales.

Asimismo, tal y como se ha indicado, el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales, lo que puede producirse o no por ausencia o deficiencia de las medidas estrictamente de seguridad.

Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita “mediante la aplicación de medidas técnicas y organizativas apropiadas”, que no son estrictamente de seguridad.

Indica I-DE 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.

Como se ha señalado anteriormente, cuando el art. 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD lo hace en el sentido previsto en el art. 25 del RGPD relativo a la privacidad desde el diseño.

Reiteramos que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Y todo ello frente a las alegaciones formuladas de contrario por I-DE que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el art. 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de disponibilidad y confidencialidad y, mediante el art. 32 del RGPD la ausencia y deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes, añadimos, que infringen el RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad y de disponibilidad.

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. Lo cual no es óbice para que, en caso de materialización de una brecha de datos personales, se considere esta circunstancia como un agravante, de conformidad con el RGPD.

Por contra, en el presente supuesto, para que estemos ante una infracción del artículo 5.1.f) ha sido y es requisito ineludible que se vulnere la confidencialidad de los datos personales (lo que no sucede con la infracción del artículo 32)

En cuanto al concurso medial, procede señalar que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD. Y ello por cuanto:

3. El RGPD es un sistema completo.

El RGPD es una norma comunitaria directamente aplicable en los Estados miembros, que contiene un sistema nuevo, completo y global destinado a garantizar la protección de datos de carácter personal de manera uniforme en toda la Unión Europea.

En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne su finalidad última que es la garantía efectiva y real del Derecho Fundamental a la Protección de Datos de Carácter Personal. Lo contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

De hecho, una muestra específica de la inexistencia de lagunas en el sistema del RGPD es el artículo 83 del RGPD que determina las circunstancias que pueden operar como agravantes o atenuantes respecto de una infracción (art. 83.2 del RGDP) o que especifica la regla existente relativa a un posible concurso medial (art. 83.3 del RGPD).

A lo anterior hemos de sumar que el RGPD no permite el desarrollo o la concreción de sus previsiones por los legisladores de los Estados miembros, a salvo de aquello que el propio legislador europeo ha previsto específicamente, delimitándolo de forma muy concreta (por ejemplo, la previsión del art. 83.7 del RGPD). La LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que este le permite y con el alcance que éste le permite.

Ello es así porque la finalidad pretendida por el legislador europeo es implantar un sistema uniforme en toda la Unión Europea que garantice los derechos y libertades de las personas físicas, que corrija comportamientos contrarios al RGPD, que fomente el cumplimiento, que posibilite la libre circulación de estos datos.

En este sentido, el considerando 2 del RGPD determina que,

"(2) *Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*". (el subrayado es nuestro)

Sigue indicando el considerando 13 del RGPED que,

"(13) *Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos*

personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". (el subrayado es nuestro)

En este sistema, lo determinante del RGPD no son las multas. Los poderes correctivos de las autoridades de control previstos en el art. 58.2 del RGPD conjugado con las disposiciones del art. 83 del RGPD muestran la prevalencia de medidas correctivas frente a las multas.

Así, el art. 83.2 del RGPD dice que "*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j)*.".

De esta forma las medidas correctivas, que son todas las previstas en el art. 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.

Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

Por ello, el art. 83.1 del RGPD previene que "Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias". (el subrayado es nuestro)

Para que dicho sistema funcione con todas sus garantías en necesario que varios elementos se desplieguen de forma íntegra y completa. La aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español-, ya sea por la aplicación de un concurso medial distinto del dispuesto en el RGPD, restaría efectividad al sistema que perdería su sentido, su finalidad teleológica, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

El RGPD está dotado de su propio principio de proporcionalidad que ha de ser aplicado en sus estrictos términos.

4. No hay laguna legal, no hay aplicación supletoria del art. 29 del RGPD.

Amén de lo expuesto, significar que no hay laguna legal respecto de la aplicación del concurso medial. Ni el RGPD permite ni la LOPDGDD dispone la aplicación supletoria de las previsiones del art. 29 de la LRJSP.

Tampoco existe aplicación subsidiaria del art. 29 del RGPD. En el Título VIII de la LOPDGDD relativo a “Procedimientos en caso de posible vulneración de la normativa de protección de datos”, el artículo 63 que abre el Título se dispone que “*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*.” Si bien existe una remisión clara a la LPACAP, no se establece en absoluto una aplicación subsidiaria respecto de la LRJSP que no contiene en su articulado disposición alguna relativa a procedimiento administrativo alguno.

De igual forma que la AEPD no está aplicando los agravantes y atenuantes dispuestos en el art. 29 de la LRJSP, puesto que el RGPD establece los suyos propios, por ende, no hay laguna legal ni aplicación subsidiaria del mismo, tampoco cabe la aplicación de apartado relativo al concurso medial y por idénticas razones.

En todo caso, los precedentes judiciales citados por la demandante sobre el concurso medial devienen de la aplicación de la LOPD del año 99 que trasponía la Directiva 95/46/CE, estableciendo el RGPD un sistema claramente distinto. En aquel momento, el artículo 115 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, sí preveía una aplicación supletoria de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del procedimiento Administrativo Común.

En tercer lugar y ya deteniéndonos en el supuesto concreto examinado, y sin perjuicio de lo antedicho, se debe destacar que no hay concurso medial. El artículo 29.5 de la LRJSP establece que “*Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*”.

Pues bien, el concurso medial tiene lugar cuando en un caso concreto la comisión de una infracción es un medio necesario para cometer otra distinta.

Los hechos constados determinan la comisión de dos infracciones distintas, sin que la conculcación del artículo 32 del RGPD (seguridad del tratamiento), tal y como asevera la parte recurrente, sea el medio necesario por el que se produce la infracción del artículo 5.1.F) del RGPD (principio de confidencialidad).

En conclusión, de todo ello y en contra de todo lo argumentado, ha quedado probado que I-DE no fue diligente por cuanto no garantizó adecuadamente la confidencialidad de los datos personales de sus clientes, así como que no contaba con las medidas técnicas y organizativas adecuadas para garantizar un nivel apropiado de seguridad.

Por lo expuesto, se desestima la alegación.

CUARTA.- SOBRE LA PRETENDIDA VULNERACIÓN POR I-DE DEL ARTÍCULO 32 DEL RGPD

Alega I-DE no estar de acuerdo en que en el Acuerdo de Inicio se indique que no fue lo suficientemente diligente a la hora de implantar medidas de seguridad apropiadas para impedir que se produjeran incidentes de seguridad como el que sucedió, pues sostiene que, tal y como ha venido poniendo de manifiesto en las respuestas dadas a la AEPD en los diferentes requerimientos de información, ha quedado acreditado que había implementado múltiples y robustas medidas de seguridad orientadas a la protección de la información de sus clientes y con anterioridad a marzo de 2022.

Procede I-DE a continuación a detallar las medidas de seguridad que tiene implantadas.

Frente a ello, se significa que en el presente caso existía una vulnerabilidad en el aplicativo web GEA, la cual fue aprovechada por el ciberdelincuente. Así, como ha quedado acreditado en los Hechos Probados y tal y como se indicó en el Fundamento de Derecho VI del Acuerdo de Inicio, ***(…).***

Por tanto, lo expuesto evidencia la existencia de un aplicativo web con una vulnerabilidad que permitía:

(…)

Asimismo, como medida posterior para evitar incidentes como el acontecido, se procedió por I-DE a modificar el aplicativo GEA ***(…)***.

Por otro lado, como medidas de seguridad existentes antes del incidente, señalaron, entre otras, las siguientes:

(…). Y es precisamente esta vulnerabilidad la que fue utilizada por el atacante durante la brecha de seguridad.

(…)

Por lo expuesto, de todo ello se deduce que este ataque se hubiera evitado si ese código no hubiera sido visible. Más aún si se tiene en cuenta que este es uno de los requisitos que se recoge en el documento indicado, ***(…).***

Asimismo, esta vulnerabilidad es identificable en las evaluaciones de seguridad. Sin embargo, durante las actuaciones de investigación I-DE no ha acreditado que detectara la vulnerabilidad de la aplicación GEA en el marco del programa de evaluación de seguridad implantado en el Grupo Iberdrola. Es más, como se ha indicado, la última revisión o evaluación de seguridad de aplicaciones críticas data de 2019, casi dos años y medio antes del incidente, por lo que no estaban siendo muy regulares teniendo en cuenta lo rápido de los avances de la tecnología, así como de la sofisticación de los ciberataques, amén de que no se ha aportado ni explicado los resultados obtenidos.

Por tanto, el aplicativo GEA contenía una vulnerabilidad evitable e identificable y que fue la aprovechada por el atacante. Ello pone de manifiesto claramente un incumplimiento del artículo 32 del RGPD, por cuanto exige medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y todo ello teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento.

(…)

En cuanto a los riesgos para los derechos y libertades en función de los cuales deben establecerse y aplicarse las medidas de seguridad apropiadas, I-DE no ha aportado un análisis de riesgos realizado con anterioridad al incidente que cumpla con el art. 32 del RGPD, pues no indica qué medidas deben aplicarse al nivel de riesgos. Asimismo, el enfoque del análisis de riesgos, contenido en el Registro de Actividades de Tratamiento respecto de la actividad afectada no está orientado a los riesgos que para los derechos y libertades de los titulares de los datos personales puede suponer la pérdida de confidencialidad, disponibilidad o de integridad.

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

Por su parte, el art. 28.2 LOPDGDD determina que "*Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:*

5. *Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.*

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales (,,,)"

Según se explica en la guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales" de la AEPD, "*El RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. El riesgo surge tanto por el tratamiento automatiza-do de datos como por su procesamiento manual, por los elementos humanos y por los recursos implicados. El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve*".

Sin embargo, no se han valorado estos riesgos. No se han valorado los daños para las personas físicas, materiales o inmateriales, o al menos no se acredita que se haya hecho, faltando, por tanto, un análisis de riesgos enfocado a la protección de los derechos y libertades de los interesados.

Por otro lado, entiende I-DE que la AEPD ha vinculado el supuesto incumplimiento del artículo 32 con la producción del resultado que se produjo como consecuencia de la concurrencia de una serie de factores que resultaban imprevisibles y que fueron detectados y solventados de forma inmediata. Concluye por ello que la AEPD está imponiendo, en lo que respecta a la adopción de medidas de seguridad, una obligación de resultado, pero que sin embargo es una obligación de medios.

A este respecto, trae a colación o manifestado por el Tribunal Supremo en su sentencia de 15 de febrero de 2022 (recurso de casación 7359/2020), que señala de forma clara que la obligación impuesta por la normativa de protección de datos personales, de adoptar medidas técnicas y organizativas encaminadas a garantizar la confidencialidad, disponibilidad e integridad de la información, es una obligación de medios y no de resultado.

A este respecto, procede señalar que la citada Sentencia efectivamente indica, sobre las medidas de seguridad en materia de protección de datos, que "… *la obligación que recae sobre el responsable y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, 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*." (el subrayado es nuestro)

Si embargo, continúa la Sentencia indicando, en el caso concreto que se analiza en la misma, que *"…el programa utilizado para la recogida de los datos de los clientes no contenía ninguna medida de seguridad que permitiese comprobar si la dirección de correo electrónico introducida era real o ficticia y si realmente pertenecía a la persona cuyos datos estaban siendo tratados y prestaba el consentimiento para ello. El estado*

de la técnica en el 1omentoo en el que se produjeron estos hechos permitía establecer medidas destinadas a comprobar la veracidad de la dirección de email, condicionando la continuación del proceso a que el usuario recibiese el contrato en la dirección proporcionada y solo desde ella prestase el consentimiento necesario para su recogida y tratamiento. Medidas que no se adoptaron en este caso.

(…) De modo que, en el momento en que se produjeron estos hechos, existían medidas técnicas referidas al proceso de registro, que hubiesen evitado la filtración de datos personales producida. Ello implica que las medidas técnicas adoptadas incumplían las condiciones de seguridad en los términos exigidos en el art. 9.1 de la LO 15/1999, incurriéndose por tanto en la infracción prevista en el art. 44.3.h) consistente en "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen […]".

Por tanto, si bien se infiere de la Sentencia que las obligaciones que establece el artículo 32 del RGPD son de medios, también deja claro que, si en el momento de producirse el incidente existían medidas técnicas adecuadas para evitar o mitigar los efectos del mismo y no fueron aplicadas, ello supone un incumplimiento de la citada obligación impuesta por el RGPD y, por ende, una infracción al mismo.

En el presente caso, como se ha señalado, existía una vulnerabilidad en el aplicativo GEA, la cual era identificable en las evaluaciones de seguridad así como evitable, tal y como lo pone de manifiesto el hecho de que posteriormente procedió I-DE a corregir dicha vulnerabilidad. Ello pone de manifiesto claramente un incumplimiento del artículo 32 del RGPD, por cuanto exige medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y todo ello teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento.

Alega asimismo I-DE que la brecha de seguridad no trae su causa de lo insuficiente de las medidas adoptadas, sino de la intensa actividad desarrollada por un tercero con la única intención de llevar a cabo el ciberataque producido en perjuicio no sólo de los clientes de i-DE, sino de la propia sociedad.

Frente a ello, debe señalarse que no 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, I-DE 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 ha indicado, existía una vulnerabilidad detectable y evitable en su aplicativo web, el cual fue aprovechado por el ciberdelincuente.

Por último, de conformidad con 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 que se valora el elemento subjetivo o culpabilístico, se insiste en que la culpabilidad de la parte actora no puede considerarse excluida ni atenuada por el hecho de que haya mediado la actuación fraudulenta de un tercero, pues la responsabilidad de la parte actora no deriva de la actuación de éste, sino de la suya propia.

Por último, señala I-DE que tenía implantados mecanismos que permitieron la detección casi inmediata de la brecha de seguridad sufrida como consecuencia del acceso a GEA, adoptando de forma inmediata, por lo que entiende i-DE que su rápida actuación es un claro ejemplo de que por la misma se daba, y se da, completo cumplimiento a lo dispuesto por el artículo 32.1 c) del RGPD, cuando se refiere a "la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico", algo que, sin embargo, no ha sido objeto de suficiente valoración por parte del Acuerdo de Inicio.

A este respecto, tanto en el Acuerdo de Inicio, como en la presente propuesta se ha tenido en cuenta que I-DE reaccionó lo más rápido posible y procedió a tomar medidas dirigidas a repeler el ataque y para evitar su repetición, considerándolo como atenuante de conformidad con el artículo 83.2.c) RGPD.

Por lo expuesto, se desestima la alegación formulada.

QUINTA. – SOBRE LA PRETENDIDA VULNERACIÓN DEL ART. 5.1.F) DEL RGPD

En este apartado I-DE alega que no se ha acreditado, ni siquiera indiciariamente, el uso fraudulento de los datos personales, limitándose el Acuerdo de Inicio a considerar que existe un riesgo muy alto ni que se haya materializado en la práctica.

A este respecto, procede aclarar que lo que se le imputa a I-DE es la vulneración del principio de confidencialidad pues consta que, tras sufrir un ataque informático contra la web GEA, aprovechando una vulnerabilidad de la misma, se produjo un acceso ilegítimo a datos personales y la extracción de los mismos por un tercero no autorizado, lo que supuso la pérdida de confidencialidad y de control de numerosos datos personales (nombre y apellidos, DNI, dirección postal, fax, e-mail, teléfono, código cliente) y que afectó a 1.350.000 clientes de I-DE. Ello supone el incumplimiento del deber de garantizar la confidencialidad de los datos personales, pues como se ha indicado, el artículo 5.1.f) señala que *deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito*.

En cuanto a que se señaló el alto riesgo de que esos datos, en manos de ciberdelincuente/s, se usaran de forma fraudulenta, ello se indicó para expresar lo que supone la pérdida de confidencialidad, pero no es necesario en modo alguno, para entender infringido el artículo 5.1.f) que dichos riesgos de uso fraudulento se materialicen, porque lo que se ha materializado con la brecha es la pérdida de confidencialidad de los datos personales tratados por I-DE, que es lo que se le imputa exclusivamente.

Por otro lado, vuelve a insistir I-DE en este apartado lo relativo a que entiende que la AEPD dio por archivada la brecha notificada por ella y que las reclamaciones no aportan nada nuevo y que, por ello, nada parece justificar la reapertura de la investigación cuando la misma había sido archivada.

A este respecto, procede remitirse a todo lo ya argumentado en relación a ello en el apartado Segundo del presente Fundamento de Derecho.

Por lo expuesto, se desestima la alegación formulada.

SEXTA. – SOBRE LA VULNERACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD

Alega I-DE que las sanciones impuestas vulneran el principio de proporcionalidad, pues la AEPD, para determinar la cuantía de las sanciones ha acudido a criterios completamente genéricos.

Así, en lo relativo a la supuesta negligencia en su actuación, indica I-DE que ha acreditado que los hechos acontecidos sucedieron en un momento concreto y que fueron solventados con total rapidez, por lo que las medidas adoptadas ante el incidente paliaron sus efectos. Esta solución inmediata de la incidencia, lo cual demuestra que sí que tenían previstas las actuaciones ante un posible ataque a sus sistemas.

Frente a ello, procede reseñar que las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que para los derechos y libertades de las personas físicas pueden tener los tratamientos de datos personales no pueden ser en modo alguno sólo medidas reactivas, es decir, para solucionar de forma inmediata una brecha de datos personales. Así, el artículo 32 del RGPD no sólo indica que deben garantizar una seguridad adecuada, sino también que dichas medidas deben incluir *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento* (letra b del artículo 32.1 RGPD). Por tanto, no basta con tener medidas para reaccionar lo antes posible cuando se ha vulnerado la confidencialidad, hay que tener también medidas previas adecuadas para impedir dicha vulneración. Y ello porque tanto o más importantes son las medidas dirigidas a salvaguardar la confidencialidad, la integridad y disponibilidad de los datos personales, es decir, las medidas preventivas dirigidas a evitar cualquier vulneración de ello.

Por tanto, no puede aceptarse que las medidas que tenía implantadas I-DE eran adecuadas por cuanto permitieron solucionar el incidente con posterioridad, pues ello sólo demuestra la existencia de medidas correctivas. No obstante, lo que permitieron esas medidas reactivas fue el cese del ataque una vez producido y la restauración del servicio, es decir, en cuanto a la protección de los datos personales evitó un impacto mayor y ello ya ha sido tenido en cuanta como atenuante en el presente procedimiento sancionador, pero en modo alguno pueden solucionar la pérdida de la confidencialidad de los datos personales afectados, por cuanto esta ya se había materializado.

Es decir, la confidencialidad de los datos personales se garantiza sobre todo con medidas preventivas. En este sentido, ya se ha indicado en la respuesta a la alegación

Cuarta del presente Fundamento de Derecho la vulnerabilidad que contenía el aplicativo GEA, que fue aprovechada por el ciberdelincuente para su ataque y que la misma, además, era perfectamente identificable en las evaluaciones de seguridad. En relación con esto último, no debe olvidarse que el artículo 32.2 RGPD determina que las medidas de seguridad deben incluir también *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*.

Por tanto, todo ello no hace sino reflejar una falta de diligencia por parte de I-DE a la hora de garantizar una seguridad adecuada al riesgo de los tratamientos de datos que lleva a cabo. En este sentido, no debe olvidarse que GEA es un aplicativo web, es decir, que permite el acceso desde internet a una base de datos donde están almacenados datos personales de millones de clientes, lo cual supone un tratamiento a gran escala, lo que exige medidas de seguridad adecuadas para ese entorno web y dirigidas especialmente a garantizar que no se produzca un acceso ilegítimo a dichos datos personales.

Por otro lado, señala I-DE no estar de acuerdo con que se considere como agravante la vinculación de su actividad con la realización de tratamientos de datos personales, pues entiende que se está agravando su conducta por pertenecer al sector eléctrico y que por ello se le debe exigir una especial diligencia, y que ello atenta de nuevo contra el principio de proporcionalidad.

Frente a ello, se significa que no se agrava su conducta por pertenecer al sector eléctrico, sino porque su actividad, el desarrollo de su negocio, supone y requiere de un continuo y abundante tratamiento de datos personales, tal y como lo demuestra el hecho de que trata datos de millones de personas.

Por tanto, como se indicó en el Acuerdo de Inicio, I-DE es una empresa habituada al tratamiento de datos personales, lo cual conlleva, de nuevo, la exigencia de un mayor grado de diligencia.

Por otro lado, se señala que el artículo 83.2 del RGPD dispone que "*Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*
(…)

> *k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso…".*

En este sentido, el legislador español ha considerado incluir en el artículo 76 de la LOPDGDD que: "2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

(…)

> *b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales."*

Esta Agencia simplemente toma en consideración esa circunstancia, prevista por el legislador, a la hora de decidir la imposición de la multa administrativa.

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 I-DE, acostumbrada al tratamiento de datos personales de millones de 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 I-DE.

Por otro lado, aduce la falta de proporcionalidad comparándolo con el expediente PS/00179/2020, en el que indica que sólo se le sancionó con 500.000 euros a pesar de que no sólo se vulneró la confidencialidad, sino que no se notificó la brecha a la AEPD, cosa que sí ha hecho I-DE, pero que, sin embargo, la sanción es considerablemente menor.

A este respecto, procede señalar, por un lado, 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.

Por otro lado, el artículo 83 establece que

> *1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.*
> *2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual*…"

Por tanto, hay que atender a las circunstancias de cada caso individual, no existiendo dos expedientes iguales y, por tanto, con resultados iguales. A modo de ejemplo, en el expediente que trae a colación los afectados fueron menos de la mitad que en el caso que nos ocupa ahora; la infracción del art. 32 del RGPD, lo fue por otro tipo de insuficiencia en las medidas para garantizar una seguridad adecuada al tratamiento; se trató de hechos acaecidos en 2018, año en que empezó a ser de obligado cumplimiento el RGPD, lo que no es lo mismo que cuatro años más tarde; no es igual el conocimiento de la técnica unos años antes y después, sobre todo por el rápido avance de la misma,v etc.

Asimismo, se señala que existen otros muchos expedientes posteriores y anteriores al presente en los que se ha sancionado con elevadas multas tanto la vulneración de la confidencialidad de los datos como la infracción de las medidas de seguridad del

artículo 32 del RGPD, aunque, como se ha señalado, debe atenderse siempre a las circunstancias concretas del caso.

Por último, y a mayor abundamiento, no procede exigir igualdad en la ilegalidad. La jurisprudencia es clara respecto a esto. Así, la Sentencia de la Audiencia Nacional de 28 de abril de 2023 (SAN 28.04.2023 REC. 409/2021 indica que "*Se alude a un trato sancionador discriminatorio puesto que esa multa o sanción económica puede sustituirse por las medidas del art. 58 RGPD, medidas menos gravosas como podría ser el apercibimiento. Y hace referencia a otras infracciones cometidas por otras entidades. Por supuesto la actora trata de comparar esta situación con otro procedimiento sancionador que se menciona, pero no estamos ante un trato discriminatorio o que se vulnere el principio de igualdad puesto que es un principio que solo opera en el marco de la legalidad cuando situaciones de hecho iguales tienen un tratamiento diferente sin justificación razonable. Como señala la STS de 20 de enero 2004, "la igualdad ha de predicarse dentro de la legalidad, de modo que si la actuación correcta de la Administración es la ahora enjuiciada, según hemos declarado, la invocada como contraria a ella no lo fue y, por consiguiente, no cabe esgrimirla para pedir que se le aplique al recurrente un trato igual, ya que, como esta Sala del Tribunal Supremo ha declarado en sus sentencias de 16 de junio de 2003 , 14 de julio de 2003 y 20 de octubre de 2003 que «el principio de igualdad carece de trascendencia para amparar una situación contraria al ordenamiento jurídico», y ello, como indica la propia Sala sentenciadora, al margen de no haberse acreditado la actuación administrativa aducida como contradictoria con la presente*".

En igual sentido señala la STS de 2 de abril de 2014 (Rec. 1916/2010) que "*la legalidad prevalece sobre una posible lesión del principio de igualdad*". *En este caso, estamos ante una infracción administrativa que se pretende comparar con otra que ha tenido diferente solución, pero de lo que se observa en la alegación que se formula por la parte actora escasamente se puede efectuar una comparación de una situación y otra. Recordemos que conforme a la doctrina constitucional consolidada para apreciar la concurrencia de una vulneración del principio de igualdad han de concurrir los siguientes presupuestos: 1) aportación de un término idóneo de comparación demostrativa de la identidad sustancial de las situaciones jurídicas que han recibido trato diferente, 2) que el trato desigual no esté fundado en razones objetivas que lo justifiquen, y 3) que el juicio comparativo se desarrolle en el marco de la legalidad, pues no cabe invocar el principio de igualdad en la ilegalidad para perpetuar situaciones contrarias a lo previsto por el ordenamiento jurídico. Así las cosas, la conducta por la que ha sido sancionada la parte actora y que es contraria a derecho no permite que su responsabilidad sea más atenuada por el hecho de que en otros supuestos, que se desconocen, la sanción impuesta no fuera económica y se considerase más beneficiosa*".

Por todo lo expuesto, se desestima la alegación formulada.

V

Respuesta a las alegaciones a la Propuesta de Resolución

En respuesta a las alegaciones presentadas por I-DE se debe señalar lo siguiente:

PRIMERA: Sobre la indefensión generada a I-DE como consecuencia de no haberse acordado la acumulación de los procedimientos EXP202305587 y EXP202205206

I-DE se ratifica de nuevo en lo alegado frente al Acuerdo de Inicio respecto de su solicitud de acumulación de ambos expedientes indicando además, que con independencia de que el artículo 57 de la LPACAP indique un “podrá”, la potestad concedida debe considerarse en todo caso exigible a la Administración cuando la tramitación no acumulada de los procedimientos pueda afectar negativamente a los derechos de los encartados en los mismos, insistiendo I-DE que la no acumulación atenta a su derecho a la defensa.

Así, indica que el expediente administrativo no contiene siquiera la acreditación real de la admisión a trámite de ninguna reclamación dirigida contra I-DE ni contra ninguna otra sociedad del Grupo Iberdrola, de forma que I-DE se ha visto obligada a intuir, a partir del Informe de Actuaciones de Investigación (IAI), la información que pudiera haber dado lugar a la apertura por la AEPD del presente procedimiento sancionador. Entiende por ello I-DE que este simple hecho resultaría suficiente para justificar la obligación de la acumulación de los dos expedientes por cuanto que su acceso a la información de que la AEPD ha dispuesto para considerar cometidas dos supuestas infracciones de la normativa de protección de datos ha quedado limitada a aquellos elementos que la AEPD ha considerado oportuno incorporar al presente expediente, sin poder tener una visión completa de hechos ni, en consecuencia, de los motivos que inducen a la AEPD a imponer tales sanciones. Por ello considera I-DE que la no acumulación de los procedimientos perjudica a sus derechos.

A este respecto, procede señalar, en primer lugar, que ya se respondió en la propuesta de resolución respecto de la solicitud de acumulación de los dos expedientes referenciados, respuesta que se encuentra transcrita en el Fundamento de Derecho III de la presente Resolución al que procede remitirse. Por tanto, si bien es cierto que es una potestad de la Administración el proceder a la acumulación o no, también lo es que se argumentaron los motivos y las razones por las cuales no procedía o no resultaba adecuado acumular ambos procedimientos sancionadores.

En cuanto lo alegado por I-DE respecto a que la no acumulación le produce indefensión, porque en su expediente no consta la admisión a trámite de ninguna reclamación contra ella, se significa que dichas admisiones a trámite tampoco constan en el otro expediente al cual solicita la acumulación, por lo que la misma no tendría efectos en este sentido, no causándole, en consecuencia, indefensión alguna la no acumulación.

A este respecto, se señala que, desde el 2 de abril de 2022, se han presentado ante esta Agencia reclamaciones de clientes afectados por el incidente de seguridad, las cuales han sido progresivamente admitidas a trámite desde el 9 de mayo de 2022. En este sentido, se indica que los reclamantes básicamente reclaman el haber visto afectados sus datos personales por la citada brecha, sin poder aportar ninguna información añadida por cuanto, como es lógico, frente a ciberataques como el sufrido, poca o nula información pueden aportar por desconocerla y no tener acceso a la misma. Dichas reclamaciones fueron admitidas a trámite de forma sucesiva, desde el 9 de mayo, por la Directora de esta Agencia, según iban presentándose desde abril de

2022. Todas ellas no han sido objeto de ningún trámite más. Es por ello por lo que dichas reclamaciones no forman parte del presente procedimiento sancionador, sólo dos a las que ha tenido acceso I-DE, por lo que no se ha causado indefensión.

Asimismo, en los Antecedentes tanto del Acuerdo de Inicio como de la Propuesta de Resolución y también de esta Resolución, se ha indicado la existencia de estas reclamaciones. Concretamente se indica en el Antecedente Quinto que "*Desde el 2 de abril de 2022, se han presentado ante esta Agencia reclamaciones de clientes afectados por el incidente de seguridad, las cuales han sido progresivamente admitidas a trámite desde el 9 de mayo de 2022*". Por tanto, a I-DE se le ha informado desde el principio de la existencia de dichas reclamaciones.

Por lo expuesto, el conocimiento o no del contenido concreto de dichas reclamaciones no afecta en modo alguno al derecho de defensa de I-DE por cuanto el presente procedimiento sancionador se inició y se ha tramitado únicamente como consecuencia de los hechos probados con ocasión de las actuaciones de investigación previa llevadas a cabo por esta Agencia. Por tanto, I-DE ha conocido en todo momento y de forma completa los hechos que se le imputan y todas las circunstancias en relación con los mismos, los cuales, se insiste, derivan exclusivamente de toda la documentación recopilada y demás actuaciones llevadas a cabo durante las investigaciones previas y no del contenido de las reclamaciones que no forman parte de ninguno de los dos procedimientos. Asimismo, ha tenido conocimiento en todo momento de las infracciones que se le imputan por tales hechos y de las sanciones que pudieran derivarse de las mismas, y ha podido alegar y presentar cuanta documentación ha considerado pertinente a lo largo del presente procedimiento sancionador.

Por tanto, la no acumulación solicitada no le produce indefensión alguna ni le afecta negativamente a ninguno de sus derechos procesales

En relación con el resto de argumentos planteados por I-DE para exigir la acumulación, al ser éstos reproducción de los expuestos frente al Acuerdo de Inicio, procede remitirse a la respuesta dada por esta Agencia y que aparece, como se ha señalado, transcrita en el Fundamento de Derecho III de la presente Resolución.

SEGUNDA: Acerca de los actos previos de la AEPD y la vulneración de los principios de buena fe, confianza legítima y seguridad jurídica.

Insiste de nuevo I-DE sobre que el escrito de 18 de abril de 2022 que se le dirigió desde la División de Innovación Tecnológica de esta Agencia tiene carácter decisorio y que ello impide o debería haber impedido cualquier actuación de investigación posterior de la brecha de datos personales sufrida lo cual, además, vulnera los principios de buena fe, confianza legítima y seguridad jurídica.

Asimismo, indica que una de las funciones de la División de Innovación Tecnológica de esta Agencia es la de "*analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la Presidencia la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción*" (artículo 31 e) del Estatuto de la AEPD).

Añade I-DE que el citado escrito viene firmado por la “AEPD”, lo cual supone que debe entenderse firmado por la Directora, pues la “representación legal e institucional” de la Agencia corresponde única y exclusivamente a la Directora, tal y como establece el artículo 13.1b) del Estatuto de la AEPD.

De ello concluye I-DE que, habiendo sido analizada por la División de Innovación Tecnológica la información comunicada por ella acerca de la brecha de seguridad, entendió que no procedía elevar a la Directora de la AEPD ningún tipo de propuesta motivada en relación con la misma, al no considerare infringido lo dispuesto en el RGPD, ello dio lugar a que esta Agencia se le notificase la decisión de no llevar a cabo actuación alguna relacionada con la citada brecha.

Frente a ello, en primer lugar procede recordar que ya se respondió a esta cuestión en la Propuesta de Resolución, respuesta que aparece transcrita enteramente en el Fundamento de Derecho IV de la presente Resolución y al que procede remitirse.

Por otro lado, no puede admitirse ni entenderse, ni siquiera de forma indirecta, que el citado escrito en cuestión se encuentra firmado por la Directora de esta Agencia, por cuanto no aparece su firma de forma expresa, por mucho que quiera I-DE presuponer de forma artificial que la firma procede de dicho órgano al ostentar la representación de la AEPD. Ninguna firma genérica de la AEPD ni de ninguno de los órganos en que se estructura, ni la firma de ninguna de las personas titulares de los mismos puede sustituir la firma de la Directora cuando ejerce las competencias que tiene atribuidas tanto por Ley como por el Estatuto de la AEPD, la delegación de firma en estos casos debe ser directa y expresa, y debe constar en el acto administrativo que se firma por delegación para garantizar y salvaguardar que la decisión ha sido adoptada por órgano competente.

En este sentido, el Estatuto de la Agencia Española de Protección de Datos, aprobado mediante Real Decreto 389/2021, de 1 de junio (en adelante el Estatuto) establece expresamente que:

1. Corresponde a la Presidencia de la Agencia Española de Protección de Datos:

> *d) Dictar las resoluciones y directrices que requiera el ejercicio de las funciones de la Agencia, en particular las derivadas del ejercicio de las competencias previstas en el artículo 57 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y del ejercicio de los poderes de investigación y de los poderes correctivos dispuestos en el artículo 58 del citado Reglamento*. (el subrayado es nuestro)

Por otra parte, el artículo 27 del Estatuto establece las competencias que tiene la Subdirección General de Inspección de Datos de la AEPD:

1. La Subdirección General de Inspección de Datos es el órgano administrativo, dependiente de la Presidencia de la Agencia Española de Protección de Datos, que desarrolla las competencias previstas en el artículo 57.1, letras f), g), h), i) y u) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y realiza las funciones de inspección y de instrucción necesarias para el ejercicio de los poderes de investigación establecidos en el artículo 58.1, letras a), b), d), e) y f)

y de los poderes correctivos dispuestos en el artículo 58.2, letras a), b), c), d), f), g), i) y j), ambos del citado Reglamento. (el subrayado es nuestro)

2. Al objeto de cumplir los cometidos establecidos en el apartado anterior, a la Subdirección General de Inspección de Datos le corresponden las siguientes funciones:

> *a) La supervisión permanente del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las disposiciones que la desarrollen, por parte de los responsables y encargados de los tratamientos.*
>
> *b) El ejercicio de las potestades de investigación definidas en el artículo 51 de la Ley Orgánica 3/2018, de 5 de diciembre.*
> *(…)*
> *d) La tramitación de los procedimientos en caso de posible vulneración de la normativa de protección de datos conforme a lo dispuesto en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, incluyendo las reclamaciones de los ciudadanos por falta de atención en sus solicitudes de ejercicio de los derechos contemplados en los artículos 15 al 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Corresponde a la Subdirección General de Inspección de Datos el deber de informar al reclamante sobre el curso y el resultado de la reclamación presentada ante la Agencia Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 77.2 del citado Reglamento.*
> *(…)*
> *e) La evaluación de la admisibilidad a trámite de las reclamaciones que se presenten ante la Agencia Española de Protección de Datos, y la propuesta a la Presidencia de decisión sobre la admisión o inadmisión a trámite, conforme a lo establecido en el artículo 65 de la Ley Orgánica 3/2018, de 5 de diciembre.*
> *(…)*
> *h) La realización de actuaciones previas de investigación acordadas por la Presidencia por propia iniciativa, a raíz de una reclamación, o a petición de otro órgano o autoridad de control, a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento, según lo dispuesto en el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre.* (el subrayado es nuestro)

Por tanto, respecto de la División de Innovación Tecnológica de la AEPD, que de conformidad con el Estatuto tiene, entre sus funciones, la de "*analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la Presidencia la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción*" (artículo 31 e) del Estatuto de la AEPD), ello no significa que sea la única y exclusiva vía por la que esta Agencia puede iniciar actuaciones de investigación. Así, esta potestad de investigación que tiene la AEPD, tal y como se ha reflejado en la normativa descrita, se lleva a cabo por la Subdirección General de Inspección de Datos, la cual, puede iniciar actuaciones de investigación bien de oficio, por orden de la Directora, bien como consecuencia de la admisión de reclamaciones presentadas ante la AEPD.

La División de Innovación Tecnológica, tras analizar la documentación aportada por I-DE (que no todas las circunstancias del incidente) ha indicado que no prevé el inicio de otras acciones, y no que no considerare infringido lo dispuesto en el RGPD o que se hubiera tomado la decisión de no llevar a cabo actuación alguna relacionada con la citada brecha. La División de Innovación Tecnológica no tomó una decisión, sino que se limitó a informar a I-DE de un pronóstico, lo que no impide que puedan tenerse en cuenta otras circunstancias, como la presentación de reclamaciones por los afectados por la brecha, que hagan aconsejable separase de esta previsión.

Por tanto, el citado escrito no tiene el carácter decisorio y resolutivo que I-DE pretende, ni por su contenido ni por su forma y ello no es óbice ni puede impedir en modo alguno la potestad de investigación que tiene la AEPD y su ejercicio a través de las funciones de inspección e investigación que la Subdirección General de Inspección de Datos tiene encomendadas. Sobre todo, tras la presentación de reclamaciones por parte de personas afectadas y que la LOPDGDD obliga a su tramitación.

Así, el artículo 65 de la LOPDGDD, relativo a la “Admisión a trámite de las reclamaciones”, establece que

> *1.Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.*
>
> *2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.*

Por tanto, presentadas reclamaciones ante la AEPD, ésta está obligada a analizar previamente su admisibilidad, pudiendo inadmitirlas únicamente en los supuestos del apartado 2 del artículo 65 transcrito, los cuales no concurrían en el caso que nos ocupa.
Por ello, una vez admitidas a trámite, se iniciaron actuaciones previas de investigación precisamente para averiguar los hechos y circunstancias acontecidas y si de los mismos se podría derivar una posible vulneración de la normativa en materia de protección de datos, tal y como permite y faculta los artículos 64 y 66 de la LOPDGDD, los cuales ya se transcribieron en la respuesta a las alegaciones al Acuerdo de Inicio y que, en aras de claridad expositiva, se vuelven a indicar:

Artículo 64. Forma de iniciación del procedimiento y duración.

> *1.Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.*
>
> *En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de*

admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2.Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

Artículo 67. Actuaciones previas de investigación.

1.Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2.Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica. (el subrayado es nuestro)

Por tanto, se reitera que de dicha normativa no se infiere en modo alguno que la AEPD tenga que justificar de la manera que exige I-DE el inicio de actuaciones previas en el sentido de que tenga que haber algo nuevo o alguna circunstancia nueva o de que las reclamaciones hayan tenido que aportar circunstancias nuevas y diferentes respecto de la documentación aportada por I-DE en su notificación de la brecha a esta Agencia, pues ello no viene exigido por la normativa indicada, además de que no se puede

pretender que los afectados aporten algo nuevo, al margen de conocer que se ha vulnerado la confidencialidad de sus datos personales por un ciberataque de cuyas circunstancias desconocen.

Precisamente las actuaciones previas de investigación se realizan para esclarecer los hechos y las circunstancias de lo acontecido, recabando más información al objeto de poder determinar o no la existencia de una posible infracción de la normativa en materia de protección de datos. En este sentido, el inicio de investigaciones previas y su realización, potestad de la AEPD con o sin reclamaciones, no prejuzga nada, sino que permite recabar la información necesaria para determinar si hay indicios o no de infracción. Incluso tras dicha investigación, puede ser que se archiven las actuaciones por entender, a la vista de la información recabada, que no existen indicios de infracción. Lo cual, en el presente caso, no ha sucedido.

Lo que sí indica la normativa reflejada es que, tras la presentación de reclamaciones, esta Agencia debe decidir si las admite a trámite o no, habiendo decidido finalmente su admisión mediante, esta vez sí, Acuerdo de admisión a trámite, firmado por la Directora de la Agencia con fecha 9 de mayo de 2022. Y, como indica el artículo 67.2 LOPDGDD referenciado, la AEPD puede llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias. Es una potestad que tiene atribuida por el RGPD y por la LOPDGDD.

Asimismo, y a mayor abundamiento de todo, tal y como se indicó, incluso en el supuesto de no haber existido las reclamaciones, la previsión de la División de Innovación Tecnológica no hubiera sido tampoco óbice ni obstáculo para el ejercicio, de oficio, de las potestades de investigación que tiene la AEPD de conformidad con el citado artículo 64.2 que determina que "*Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación…*"

Por tanto, el presente procedimiento sancionador no se ha iniciado por el contenido o por alguna información nueva aportada en las reclamaciones, sino por la información y documentación obtenida tras el período de actuaciones previas de investigación, al inferirse de la misma posibles vulneraciones a la normativa en materia de protección de datos.

TERCERA: Sobre los argumentos sostenidos por la Propuesta de Resolución para considerar que no concurre *bis in ídem*.

Vuelve a indicar I-DE que se ha vulnerado el principio *non bis in ídem* en la imposición de las dos infracciones, pues entiende que la AEPD no está enjuiciando la vulneración del artículo 5.1.f) del RGPD por un motivo distinto del derivado de la, a su juicio, inadecuada seguridad de los datos personales, sino única y exclusivamente por ese motivo.

A este respecto, ya se señaló la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017), que dispone,

"(…) Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.

Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):

> *a) La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.*
>
> *b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.*
>
> *c) La identidad de fundamento o causal, implica que las medidas sancionadoras no pueden concurrir si responden a una misma naturaleza, es decir, si participan de una misma fundamentación teleológica, lo que ocurre entre las penales y las administrativas sancionadoras, pero no entre las punitivas y las meramente coercitivas*."

Tomando como referencia lo anteriormente explicitado en el procedimiento sancionador no se ha vulnerado el principio non bis in ídem, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una brecha de datos personales, la infracción del art. 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad que afectó a unos determinados clientes, la infracción del art. 32 del RGPD se reduce a la deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la brecha de datos personales. De hecho, si estas medidas de seguridad que tenía implantadas I-DE se hubieran detectado por la AEPD sin que se hubiera producido la pérdida de confidencialidad, únicamente habría sido sancionada por el art. 32 del RGPD.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de confidencialidad y disponibilidad y mediante el art. 32 del RGPD la deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad deficientes, añadimos, que infringen el RGPD, independientemente de que se hubiera o no producido la brecha de datos personales.

El artículo 32 del RGPD se vulnera con independencia de si se produce o no una brecha de datos personales. Es decir, se infringe por no tener medidas apropiadas para garantizar una adecuada seguridad en el tratamiento de los datos sin que para ello sea necesario o imprescindible que se produzca una brecha de seguridad de los datos personales que, en su caso, pueda afectar bien a la confidencialidad de los

datos, bien sólo a la disponibilidad, o sólo a la integridad, o a algunas o a todas ellas. Otra cosa es que la deficiencia en las medidas de seguridad se ponga de manifiesto, en el caso concreto, con ocasión de una violación de la seguridad de los datos personales (vulneración de la confidencialidad en este caso), como ha ocurrido en el presente supuesto.

Por otro lado, el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad o de integridad de los datos personales, lo que puede producirse o no por ausencia o deficiencia de las medidas de seguridad. Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita “mediante la aplicación de medidas técnicas y organizativas apropiadas”, que no son estrictamente de seguridad.

Asimismo, se significa nuevamente que el artículo 5.1.f) del RGPD es uno de los principios relativos al tratamiento. Los principios relativos al tratamiento son, por un lado, el punto de partida y la cláusula de cierre del ordenamiento jurídico de protección de datos, constituyendo verdaderas reglas informadoras del sistema con una intensa fuerza expansiva; por otro lado, al tener un alto nivel de concreción, son normas de obligado cumplimiento susceptibles de ser infringidas.

La vulneración de la confidencialidad que se imputa a I-DE 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.

Por último, procede añadir que, en relación con la supuesta vulneración del principio de *non bis in ídem*, ya se dio respuesta sobre esta alegación en la Propuesta de Resolución, en la que de forma extendida se argumenta la no existencia de la triple identidad de hechos, sujeto y fundamento, tal y como exige la jurisprudencia, respuesta que aparece totalmente transcrita en apartado Tercero del Fundamento de Derecho IV de esta Resolución y al que procede remitirse.

Por último, en cuanto a lo alegado por I-DE relativo a que en la imputación de la infracción del artículo 5.1.f) se está exigiendo una obligación de resultado, lo que resulta contrario a la Sentencia de 15 de febrero de 2022 (recurso de casación 7359/2020), que señala que la obligación impuesta por la normativa de protección de datos personales, de adoptar medidas técnicas y organizativas es una obligación de medios y no de resultado, se significa, que lo analizado en dicha Sentencia es el cumplimiento de las medidas técnicas y organizativas en el sentido de si son adecuadas para garantizar la seguridad de los tratamientos, es decir, que estaríamos no en el ámbito del cumplimiento del artículo 5.1.f, sino en el ámbito del cumplimiento del artículo 32 RGPD al tratarse de medidas de seguridad. Por tanto, el argumento dado por I-DE y el análisis del mismo que se va a realizar han de referirse exclusivamente en relación con la infracción del artículo 32 RGPD, el cual se va a desarrollar en el apartado Quinto del presente Fundamento de Derecho relativo a la infracción del artículo 32.

CUARTA: Sobre la aplicación de los principios del derecho sancionador a la actividad de la AEPD y la concurrencia de un concurso medial.

Alega de nuevo I-DE que, en el caso de no apreciarse la existencia del *bis in idem*, al menos una de las infracciones se encontraría subsumida y embebida en la otra, ya que la imputación de la infracción del artículo 5.1.f) del RGPD se debe a que el tratamiento no se ha llevado a cabo, a juicio de la AEPD, cumpliendo con las necesarias medidas de seguridad. Entiende por tanto I-DE la existencia de absoluta vinculación entre la supuesta ausencia de medidas de seguridad adecuadas y la quiebra del principio de confidencialidad. Es decir, que es la supuesta insuficiencia de las medidas de seguridad la que directamente conduce a la vulneración del artículo 32 y a la vulneración del 5.1.f).
Existiendo, por tanto, un claro supuesto de concurso medial, pues las dos infracciones imputadas no pueden cometerse la una sin la otra.

A continuación, argumenta I-DE las razones por las que considera que sí es de aplicación el artículo 29 de la LRJSP y que, con su no aplicación, la AEPD está derogando implícitamente, en materia de protección de datos, de todas las garantías del régimen sancionador establecidas por el Tribunal Constitucional.

A este respecto, como quiera que esta alegación ya se formuló frente al Acuerdo de Inicio y que la misma fue ampliamente respondida en la Propuesta de Resolución, la cual se transcribe íntegramente en el apartado Tercero del Fundamento de Derecho IV, procede remitirse a ello en su totalidad.

Por otro lado, en relación con la mención que realiza la AEPD respecto a la no aplicabilidad del art. 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, “LRJSP”), I-DE trae a colación el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, en cuyo artículo 3 se establece que la AEPD se rige por lo dispuesto en el RGPD, y supletoriamente, por la LRJSP. Entiende I-DE que lo anterior viene a implicar que, en relación con todo aquello no regulado expresamente en el RGPD o la LOPDGDD se atenderá a lo previsto al efecto en la LRJSP, como es el caso de los concursos de infracciones previstos en el artículo 29 del LRJSP en relación con el principio de proporcionalidad como principio de la potestad sancionadora.

Frente a ello, se significa que el artículo 3.2 del citado Estatuto de la AEPD establece lo siguiente:

> *2. Supletoriamente, en cuanto sea compatible con su plena independencia, se regirá por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en particular lo dispuesto para organismos autónomos; por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; por la Ley 47/2003, de 26 de noviembre, General Presupuestaria; por la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014; por la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, así como el resto de las normas*

> *de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común.*

Por tanto, lo que se está indicando es que se le aplica supletoriamente el régimen jurídico del Sector Público, pero en lo relativo a su consideración como organismo público perteneciente a la Administración General del Estado, es decir, a consideraciones como su composición, organización, estructura, etc.

Por su parte, en el artículo 3.3 del Estatuto de la AEPD se indica lo siguiente:

> *3. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.*

Por tanto, en los procedimientos tramitados por ella, entre ellos, el procedimiento sancionador, no se aplica supletoriamente ni la LRJSP ni la LPAC, sino que declara que los procedimientos tramitados por la AEPD se regirán por el RGPD y la LOPDGDD. Y con carácter subsidiario (que no supletorio) por las normas sobre los procedimientos administrativos.

A este respecto, se insiste en que no hay aplicación supletoria del citado precepto, por cuanto no hay laguna legal al respecto de la aplicación del concurso medial previsto en dicho artículo 29 de la LRJSP. Ni el RGPD permite ni la LOPDGDD dispone la aplicación supletoria de las previsiones del art. 29 de la LRJSP.

En el Título VIII de la LOPDGDD relativo a “Procedimientos en caso de posible vulneración de la normativa de protección de datos”, el artículo 63 que abre el Título se dispone que "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*.". Si bien existe una remisión a la LPACAP, no se establece en absoluto una aplicación subsidiaria respecto de la LRJSP que no contiene en su articulado disposición alguna relativa a procedimiento administrativo alguno.

De igual forma que la AEPD no está aplicando los agravantes y atenuantes dispuestos en el mismo art. 29 de la LRJSP, puesto que el RGPD establece los suyos propios, por ende, no hay laguna legal ni aplicación subsidiaria del mismo, tampoco cabe la aplicación de apartado relativo al concurso medial y por idénticas razones.”

Como ya se indicó, además la aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español-, ya sea por la aplicación de un concurso medial distinto del dispuesto en el RGPD, restaría efectividad al sistema que

perdería su sentido, su finalidad teleológica, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

Aclarar, con carácter previo que, la supletoriedad se refiere a supuestos en los que en una determinada norma no se regula un específico supuesto, laguna legal, dando lugar a la aplicación de otra norma jurídica que regule tal situación, siempre que no resulte disconforme con el ordenamiento jurídico.

Mientras que la subsidiaridad hace referencia a un concurso de normas, lo que supone que para un determinado supuesto pueden ser aplicables dos o más normas, de manera que la norma subsidiara cede en beneficio de la principal.

Pues bien, examinados tanto la supletoriedad como la subsidiariedad, se concluye la no aplicación del artículo 29 de la LRJSP sino del artículo 83 del RGPD en relación con el principio de proporcionalidad.

Ello es así por cuanto:

• El principio de proporcionalidad se aplica al procedimiento sancionador.

• El principio de proporcionalidad se regula de forma completa en el artículo 83 del RGPD.

• No hay laguna legal.

• Ni el RGPD ni la LOPDGDD remiten a la aplicación, por existencia de laguna legal, del artículo 29 de la LRJSP.

• En los procedimientos tramitados por la AEPD, para los procedimientos administrativos tramitados, se prevé la aplicación subsidiaria de las normas generales sobre los procedimientos administrativos.

• En los procedimientos tramitados por la AEPD, para los procedimientos administrativos tramitados y no en relación con los principios del procedimiento sancionador, no se establece en la LOPDGDD una aplicación subsidiaria de la LRJSP.

Por tanto, no hay ni supletoriedad ni subsidiaridad que hagan que se aplique el artículo 29 de la LRJSP.

En cuanto al hecho de que, tal y como indica I-DE, la propia Agencia anteriormente ha considerado aplicable dicho artículo 29 considerando la existencia de supuestos de concurso medial, como en su Resolución de 23 de abril de 2021, dictada en el procedimiento PS/00240/2019, procede señalar que la Administración puede separarse de lo resuelto con anterioridad. Así, el artículo 35 de la LPACAP establece que:

1. Serán motivados, con sucinta referencia de hechos y fundamentos de derecho:

> *c) Los actos que se separen del criterio seguido en actuaciones precedentes o del dictamen de órganos consultivos.*

Por tanto, es legítimo que la Administración se separe del criterio seguido en actuaciones precedentes, siempre y cuando dicho cambio esté motivado, lo cual concurre en el presente caso. Así, además de lo que se acaba de argumentar en este propio apartado, procede recordar de nuevo que ya se formuló esta alegación frente al Acuerdo de Inicio, relativa al concurso medial y se respondió al mismo motivando y argumentando por qué no se considera la existencia del concurso medial y, además, se motiva la no aplicabilidad del artículo 29 LRJSP. Por tanto, procede remitirse a los argumentos esgrimidos y que aparecen transcritos en el apartado Tercero del Fundamento de Derecho IV de la presente Resolución.

Por tanto, una vez argumentado y motivado no sólo que no se considera la existencia de concurrencia de infracciones, así como las razones por las cuales no se considera aplicable el artículo 29 LRJSP, resulta legítimo y no contrario a derecho el cambio de criterio.

En este sentido, la Sentencia de 12 de marzo de 2018, del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso administrativo, Sección 4ª (Rec. 761/2017), señala, con ocasión de la revisión de un procedimiento sancionador, que:

> *"(…) la Administración puede separarse de lo resuelto con anterioridad motivando el cambio (art. 35.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas). Como señala el Tribunal Supremo en su Auto de 4 de diciembre de 1998 "... para que la doctrina de los actos propios de la Administración tenga aplicación es necesario fundamentalmente que un primer órgano de la Administración haya dictado un primer acto declarativo de derechos y luego que en el segundo revoque la decisión tomada en el primero", y dicha circunstancia no concurre en este caso porque el presente acto administrativo de liquidación tributaria no revoca ninguna decisión tomada en un acto precedente relativo al mismo concepto tributario ni existe un acto declarativo expreso que ahora se modifique.*
>
> *A estos efectos, procede distinguir entre la eficacia de los actos propios de la Administración y la vinculación de la Administración a los precedentes interpretativos aplicados en situaciones anteriores ya que, en el supuesto que se cuestiona, y empleando palabras del Tribunal Supremo (sentencia de 25 de febrero de 2000), no cabe hablar de "acto propio sino a lo más cambio de criterio e interpretación, lo cual es perfectamente válido ". Igualmente, la STS de 27 de junio de 2000 refiere:*
>
> *"... el principio de actuar contra los propios actos no podría llevarse a extremos tales que obstaran a la conformidad a Derecho de una determinada actuación, por el mero hecho de» (la existencia de) «otra anterior de distinto signo aunque ésta no se amparara en la legalidad, del mismo modo que la igualdad sólo cabe dentro del ámbito de la legalidad, tal como es suficientemente conocido,*

so pena de poder consolidar para siempre resoluciones ilegales o no ajustadas a Derecho, irreversibles y de imposible modificación ulterior».

En el mismo sentido se ha expresado el Alto Tribunal en otras Sentencias. Así, en la de 1 de febrero de 1999 , declara que «este principio no puede invocarse para crear, mantener o extender en el campo del Derecho público, situaciones contrarias al ordenamiento jurídico, o cuando el acto precedente resulta en contradicción con el fin o el interés tutelado por una norma jurídica que, por su naturaleza, no es susceptible de amparar una actuación discrecional de la Administración que suponga el reconocimiento de unos derechos y/u obligaciones que dimanen de actos propios de la misma. O dicho de otro modo, la doctrina de los actos propios sin la limitación que acaba de exponerse podría introducir en el ámbito de las relaciones de Derecho público el principio de la autonomía de la voluntad como método ordenador de materias reguladas por normas de naturaleza imperativa, en las que prevalece el interés público salvaguardado por el principio de legalidad; principio que resultaría conculcado si se diera validez a una actuación de la Administración contraria al ordenamiento jurídico por el sólo hecho de que así se ha decidido por la Administración o porque responde a un precedente de ésta. (...) o, dicho en otros términos, no puede decirse que sea legítima la confianza que se deposite en un acto o precedente que sea contrario a la norma imperativa" (el subrayado es nuestro).

Asimismo, y a mayor abundamiento, este criterio de entender no aplicable el artículo 29 LRJSP no es nuevo pues se ha aplicado en expedientes sancionadores anteriores al presente. A modo de ejemplo, se señala el PS/00020/2023 y PS/00667/2023.

Por último, I-DE alega que la aplicación del artículo 29 es una posibilidad asimismo reconocida por las Directrices 4/2022, sobre el cálculo de multas administrativas bajo el RGPD, donde expresamente se estipulan los criterios que debe seguir la autoridad administrativa para evaluar, de forma previa a la imposición de la sanción, la posible concurrencia de estas.

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."

Asimismo, en este momento hemos de recordar que la gravedad de las infracciones del RGPD se determina en atención a las reglas establecidas en este y no en la LOPDGDD. La tipificación de las infracciones se encuentra regulada en el artículo 83, apartados 4, 5 y 6 del RGPD, mientras que la calificación de las infracciones como muy graves, graves o leves a los solos efectos de la prescripción se dispone en los artículos 72, 73 y 74 de la LOPDGDD.

Por último y no menos importante, la AEPD no sanciona por una misma ofensa, como aduce I-DE, sino que se han constatado a través de hechos probados no rebatidos por I-DE, la comisión de dos infracciones diferenciadas, tipificadas de forma diferenciada, no existiendo, además, en el caso concreto, concurso medial.

Por todo lo expuesto, se desestima la presente alegación.

QUINTA: Sobre la inexistencia de vulneración por I-DE del artículo 32 del RGPD

Indica de nuevo I-DE había llevado a cabo un análisis de los riesgos que el tratamiento de los datos a partir del acceso a GEA podía generar en los derechos y libertades de los interesados, así como implementado medidas de seguridad que permitían mitigar los mencionados riesgos

No está de acuerdo I-DE sobre que esta Agencia entienda que las medidas de seguridad resultaban insuficientes por haberse constatado la existencia de una vulnerabilidad en GEA que ha dado lugar a la brecha de datos personales, por cuanto entiende que las medidas adoptadas por I-DE eran robustas a pesar de haber existido un incidente de seguridad, lo cual no niega, pero sí que niega que pueda considerarse que este resultado ha de determinar necesariamente la insuficiencia de las medidas adoptadas por I-DE.

Señala asimismo I-DE que, aun cuando la AEPD pretenda indicar que la vulnerabilidad finalmente detectada era "evitable e identificable", lo cierto es que la misma no lo había sido a pesar de la adopción por i-DE de la totalidad de las directrices establecidas por el Grupo Iberdrola para preservar la seguridad de la información objeto de tratamiento, como del mismo modo tampoco resultaba "evitable e identificable" que se produjera un compromiso en las credenciales de un usuario de GEA ***(…)***, tal y como indican las conclusiones del informe forense aportado por mi representada (folio 519 del expediente administrativo), sin que en ningún caso se haya podido acreditar que la exfiltración tuviera lugar como consecuencia del modo en que se hubiera establecido la generación de contraseñas en el aplicativo, como afirma rotundamente la AEPD.

Y en este sentido, entiende I-DE que es obvio indicar que el estado del arte de las técnicas de *pentesting* no garantiza al cien por cien la detección de todas y cada una de las vulnerabilidades, que ni pueden ser calificadas, como parece considerar la AEPD de evidentes, ni aún menos considerarse "evitable[s] e identificable[s]".

Sostiene por ello que el razonamiento sostenido por la AEPD sólo puede ser calificado de circular porque, siendo manifiesto que la jurisprudencia ha puesto de relieve que la

obligación de adopción de las medidas de seguridad es de medios y no de resultado, la AEPD realiza una valoración del supuesto incumplimiento por I-DE de la obligación de implementar medidas de seguridad invirtiendo el razonamiento que ha de seguirse para ello, al indicar a lo largo de su Propuesta de Resolución que, en definitiva las medidas eran objetivamente inadecuadas como consecuencia del hecho de que efectivamente se pudo producir el ataque y la brecha de seguridad tuvo lugar.

Sostiene por ello I-DE que, de este modo, la AEPD pretende eludir la doctrina sustentada por el Tribunal Supremo en su sentencia de 15 de febrero de 2022 haciendo referencia a la insuficiencia de las medidas, pero en definitiva su razonamiento es que el resultado es tomado en consideración como premisa para considerar que los medios eran inadecuados antes de que se produjera.

Por ello reitera I-DE todo lo indicado en el escrito de alegaciones al Acuerdo de Inicio y traer nuevamente a colación la sentencia del Tribunal Supremo que acaba de mencionarse, toda vez que la AEPD pretende únicamente crear una apariencia de que el resultado no es tomado en consideración como hecho determinante de la supuesta infracción del artículo 32, cuando, como se ha acreditado, dicho resultado es la premisa en que la AEPD funda la supuesta insuficiencia de las medidas adoptadas por mi representada.

Frente a ello, procede indicar, en primer lugar, que el análisis de los riesgos del tratamiento realizado a partir del acceso desde la aplicación GEA no muestra medida alguna a adoptar para paliar los supuestos riesgos detectados. De hecho, es un análisis basado en un documento adjuntado por I-DE como *Documento Nº 8 documento explicativo de la lógica seguida para el cálculo del nivel de riesgo conforme a esta metodología. Dicha metodología se encuentra implantada de forma automatizada en la propia herramienta corporativa de registro de actividades de tratamiento, de forma que en el propio proceso de registro determina el nivel de riesgo del tratamiento. Así pues, la aplicación de dicha metodología en relación con el tratamiento ***TRATAMIENTO.1 arrojó como resultado un nivel de riesgo MEDIO, como se recoge en el Documento Nº 7 arriba referido"*.

En el citado Documento 8 se detallan ciertas amenazas o circunstancias como "colectivos vulnerables" "acceso a los datos personales por más de 10 personas" "transferencias internacionales" "tratamientos a gran escala" "perfiles con efectos jurídicos". Estas circunstancias se establecen como preguntas y, según se responda "si" o "no", se le aplica un resultado:

(…)

Varias de estas preguntas aparecen en el Documento 7 referenciado por I-DE, que parece ser el Registro de Actividades de Tratamiento de la actividad afectada por la brecha de datos personales, en las que se contesta "Sí" o "No" y de ello se indica un riesgo "Medio", pero nada más. Es decir, no se indica medida alguna adoptada o que deba ser adoptada para paliar ese riesgo medio. Ni si se trata de un riesgo inherente o de un riesgo residual.

Asimismo, tal y como se le indicó en la Propuesta de Resolución en respuesta a esta misma alegación, tampoco, a la vista del citado Documento 8, dicho análisis está

enfocado a los riesgos de probabilidad y gravedad variables que para los “derechos y libertades de las personas físicas puede conllevar el tratamiento, como pueden ser daños y perjuicios físicos, materiales o inmateriales, en particular problemas de discriminación, usurpación de identidad, fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados, etc, todo ello de conformidad con el Considerando 75 del RGPD

Por su parte, el art. 28.2 LOPDGDD determina que “*Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:*

> *a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.*
>
> *b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales (,,,)”*

Asimismo, según se explica en la guía “Gestión del riesgo y evaluación de impacto en tratamientos de datos personales” de la AEPD, “*El RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. El riesgo surge tanto por el tratamiento automatizado de datos como por su procesamiento manual, por los elementos humanos y por los recursos implicados. El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve*”.

Sin embargo, tal y como ya se le indicó, no se han valorado estos riesgos. No se han valorado los daños para las personas físicas, materiales o inmateriales, o al menos no se acredita que se haya hecho, faltando, por tanto, un análisis de riesgos enfocado a la protección de los derechos y libertades de los interesados. Asimismo, tampoco se indica qué medidas de seguridad a adoptar para paliar ese riesgo “Medio” arrojado.

Por tanto, I-DE no ha acreditado lo que manifiesta respecto de que “*había llevado a cabo un análisis de los riesgos que el tratamiento de los datos a partir del acceso a*

GEA podía generar en los derechos y libertades de los interesados, así como implementado medidas de seguridad que permitían mitigar los mencionados riesgos"

En segundo lugar, en cuanto a que I-DE tenía implementadas medidas robustas y que esta Agencia ha vinculado el supuesto incumplimiento del artículo 32 al resultado del incidente, trayendo de nuevo a colación lo manifestado por el Tribunal Supremo en su sentencia de 15 de febrero de 2022 (recurso de casación 7359/2020), se significa que, tal y como ya se le respondió a esta misma alegación en la Propuesta de Resolución, las deficiencias detectadas y que suponen el incumplimiento del artículo 32 del RGPD existían con independencia del ataque y de la brecha de seguridad acaecida.

Así, en el presente caso existía una vulnerabilidad en el aplicativo web GEA, de forma previa al ataque y la cual fue aprovechada por el ciberdelincuente. Así, como ha quedado acreditado en los Hechos Probados, el ataque se produjo desde un usuario válidamente logado ***(…).***

Por tanto, lo expuesto evidencia la existencia de un aplicativo web con una vulnerabilidad que permitía:

-(…)

Asimismo, como medida posterior para evitar incidentes como el acontecido, se procedió por I-DE a modificar el aplicativo GEA ***(…)***.

Por otro lado, como medidas de seguridad existentes antes del incidente, señalaron, entre otras, las siguientes:

(…). Y es precisamente esta vulnerabilidad la que fue utilizada por el atacante durante la brecha de seguridad.

(…).

Por lo expuesto, de todo ello se deduce que este ataque se hubiera evitado si ese código no hubiera sido visible. Más aún si se tiene en cuenta que este es uno de los requisitos que se recoge en el documento indicado, ***(…).***

Asimismo, esta vulnerabilidad es identificable en las evaluaciones de seguridad. Sin embargo, durante las actuaciones de investigación I-DE no ha acreditado que detectara la vulnerabilidad de la aplicación GEA en el marco del programa de evaluación de seguridad implantado en el Grupo Iberdrola. Es más, como se ha indicado, la última revisión o evaluación de seguridad de aplicaciones críticas data de 2019, casi dos años y medio antes del incidente, por lo que no estaban siendo muy regulares teniendo en cuenta lo rápido de los avances de la tecnología, así como de la sofisticación de los ciberataques, amén de que no se ha aportado ni explicado los resultados obtenidos.

Por tanto, el aplicativo GEA contenía una vulnerabilidad evitable e identificable y que fue la aprovechada por el atacante. Ello pone de manifiesto claramente un incumplimiento del artículo 32 del RGPD, por cuanto exige medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y todo ello teniendo en cuenta el

estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento.

(…)

Por tanto, todo ello pone de manifiesto que las medidas de seguridad en el momento del incidente no eran las apropiadas para una protección adecuada de los datos personales según los riesgos de los tratamientos y teniendo en cuenta el estado de la técnica y a los costes del momento.

Por lo expuesto, en modo alguno se ha señalado por esta Agencia que la exfiltración tuviera lugar como consecuencia del modo en que se hubiera establecido la generación de contraseñas en el aplicativo afectado. Lo que se ha señalado es que el ataque tuvo lugar habiéndose aprovechado la vulnerabilidad en dicho aplicativo consistente en la visualización, a partir de una sesión validada de forma correcta***, (…).***

Además de este hecho, lo que se ha señalado por esta Agencia es que también existían otras deficiencias en las medidas de seguridad, como una política de contraseñas ***(…).***

Ello son deficiencias en sí mismas, con independencia, se insiste, del concreto incidente acaecido y de la brecha de datos personales ocurrida. No obstante, no puede obviarse el hecho de que la vulnerabilidad en el aplicativo GEA fue precisamente la aprovechada por el atacante que, además consiguió inicialmente acceder válidamente logado sin que se detectara en un primer momento la exfiltración ilegítima de información y sin que se haya podido saber con total seguridad por qué medio consiguió las credenciales de un usuario, pues en el informe emitido por la empresa SIA sobre el incidente, se indica que:

(…)

Asimismo, la propia empresa SIA, en sus recomendaciones expresamente indicó:

• ***(…)***

En cuanto a la posibilidad de accesos a la aplicación web desde IP sospechosas o maliciosas o, al menos, no necesarias para el negocio, no debe olvidarse tampoco que, tal y como se señaló en el informe de la empresa SIA, ***(…).***

Por tanto, en modo alguno se ha basado esta Agencia en el resultado del ciberataque para justificar el incumplimiento del artículo 32 del RGPD, por cuanto, tal y como se ha señalado, dicho incumplimiento ya se producía antes y con independencia de ataque sufrido, lo cual pone en evidencia que no se contaba con las medidas apropiadas para garantizar un nivel de seguridad adecuado.

Por último, en cuanto a la Sentencia del Tribunal Supremo de 15 de febrero de 2022 (recurso de casación 7359/2020), indicada por I-DE, se significa, tal y como ya se señaló en la Propuesta de Resolución, que la citada Sentencia efectivamente indica, sobre las medidas de seguridad en materia de protección de datos, que "… *la obligación que recae sobre el responsable y sobre el encargado del tratamiento*

respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, 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." (el subrayado es nuestro)

Si embargo, continúa la Sentencia indicando, en el caso concreto que se analiza en la misma, que *"…el programa utilizado para la recogida de los datos de los clientes no contenía ninguna medida de seguridad que permitiese comprobar si la dirección de correo electrónico introducida era real o ficticia y si realmente pertenecía a la persona cuyos datos estaban siendo tratados y prestaba el consentimiento para ello. El estado de la técnica en el momento en el que se produjeron estos hechos permitía establecer medidas destinadas a comprobar la veracidad de la dirección de email, condicionando la continuación del proceso a que el usuario recibiese el contrato en la dirección proporcionada y solo desde ella prestase el consentimiento necesario para su recogida y tratamiento. Medidas que no se adoptaron en este caso.*

(…) De modo que, en el momento en que se produjeron estos hechos, existían medidas técnicas referidas al proceso de registro, que hubiesen evitado la filtración de datos personales producida. Ello implica que las medidas técnicas adoptadas incumplían las condiciones de seguridad en los términos exigidos en el art. 9.1 de la LO 15/1999, incurriéndose por tanto en la infracción prevista en el art. 44.3.h) consistente en "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen [...]".

Debe señalarse, en primer lugar, que esta sentencia se dicta al amparo de la normativa anterior al RGPD, en la que, conforme al sistema previsto en la LOPD y en el RLOPD, las medidas de seguridad estaban perfectamente estandarizadas. Se ha pasado de un sistema con medidas de seguridad estándar y estáticas para cualquier responsable a medidas de seguridad propias para cada organización (adaptadas a sus características e idiosincrasia), que considera los riesgos específicos de la entidad de que se trate; además ahora son dinámicas, de tal forma que no se agota con la implementación de las medidas de seguridad adecuadas al riesgo al inicio de los tratamientos, sino que debe de ir adaptándose a los riesgos que vayan apareciendo.

La nueva regulación prevista en el RGPD amplía notablemente las obligaciones del responsable del tratamiento y su ámbito de acción y responsabilidad, extendiéndose ahora de manera clara a las actuaciones realizadas por sus encargados del tratamiento, que quedan dentro de su ámbito de responsabilidad.

En segundo lugar, la Sentencia del Tribunal Supremo citada considera, en relación con una infracción del art. 9 de la LOPDP que "*la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de*

medidas técnicas y organizativas, 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".

Sobre ello precisa que "*No basta con diseñar los medios técnicos y organizativos necesarios también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de la diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso*".

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, incluso 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 I-DE 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".

Por tanto, si bien se infiere de la Sentencia que las obligaciones que establece el artículo 32 del RGPD son de medios, también deja claro que, si en el momento de producirse el incidente existían medidas técnicas adecuadas para evitar o mitigar los efectos del mismo y no fueron aplicadas, ello supone un incumplimiento de la citada obligación impuesta por el RGPD y, por ende, una infracción al mismo.

En el presente caso, como se ha señalado repetidamente, existía una vulnerabilidad en el aplicativo GEA, ***(…).*** Ello pone de manifiesto claramente un incumplimiento del artículo 32 del RGPD, por cuanto exige medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y todo ello teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento.

Por lo expuesto, se desestima la alegación.

SEXTA: Sobre la inexistencia de vulneración del principio de confidencialidad e integridad.

Reseña de nuevo I-DE la absoluta identidad entre las dos infracciones que se le imputan hasta el punto de que la supuesta vulneración del artículo 5.1.f) del RGPD o bien resulta ser el resultado de la supuesta vulneración del artículo 32 de dicho Reglamento o bien trae causa directa, inmediata y exclusiva de este supuesto segundo incumplimiento, es decir por la falta de medidas de seguridad adecuadas.

Señala I-DE a este respecto que no se ha considerado por la AEPD la existencia de vulneración alguna que no se refiera a las medidas de seguridad, pues no se ha

indicado ninguna medida que haya dejado de cumplir distintas a las de seguridad que puedan ser exigibles.

A este respecto, ya se indicó en la Propuesta de Resolución que cuando el art. 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD lo hace en el sentido previsto en el art. 25 del RGPD relativo a la privacidad desde el diseño.

Este precepto determina que,

> "*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados*" (el subrayado es nuestro)

Debe señalarse que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

En este sentido, I-DE no ha acreditado que haya cumplido con lo establecido en dicho precepto, puesto que no se ha acreditado que, de conformidad con los riesgos de diversa probabilidad y gravedad que entraña el tratamiento, para los derechos y libertades de las personas físicas, haya aplicado medidas técnicas y organizativas apropiadas como por ejemplo, la seudonimización, concebidas y dirigidas a aplicar de forma efectiva los principios de protección de datos, entre los que se encuentra el principio de confidencialidad.

Por tanto, el RGPD exige la aplicabilidad de la protección de datos desde el diseño y la necesidad de gestionar tanto los riesgos para los derechos y libertades de los individuos, como el impacto para esos derechos y libertades que podría tener una brecha de datos, sobre todo en entornos web, debido a que pueden afectar a un gran volumen de población.

Según se recoge en las orientaciones para tratamientos que implican comunicación de datos entre administraciones públicas de esta Agencia, cuyos razonamientos resultan extrapolables a grandes organizaciones que manejen gran cantidad de datos, siempre existen riesgos relacionados con las brechas de datos personales. Sin embargo, estos serán especialmente considerables en tratamientos de datos personales llevados a cabo por grandes organizaciones públicas y privadas que estén dando servicio a gran parte de los ciudadanos, y aun mucho más si están interconectadas. Es muy importante tener en cuenta que el riesgo que pueden suponer brechas de datos

personales en dichos tratamientos no depende tanto de que se traten categorías de datos sensibles y/o especialmente protegidos como de las consecuencias para los derechos fundamentales que se pueden derivar de un compromiso de la información

Para estimar el impacto que pudiera tener una brecha de datos personales hay que plantearse las consecuencias que se derivarían de su materialización. Una forma de hacerlo es, antes que se produzca una brecha, plantearse los posibles escenarios de materialización de un compromiso de los datos personales, determinar sus consecuencias, y evaluar cómo afecta a los derechos y libertades de los interesados, sobre todo si se trata de consecuencias irreversibles en sus derechos fundamentales

En cuanto a las medidas apropiadas al nivel de riesgos para los derechos y libertades, el art. 24.1 del RGPD establece que las medidas que se han de adoptar en un tratamiento para garantizar y poder demostrar su conformidad con el Reglamento deben tener en cuenta el ámbito, el contexto y los fines del tratamiento, debiendo atender, en particular, a la extensión de sujetos afectados por el mismo y al riesgo que supone para los derechos fundamentales y no sólo la tipología de los datos

En las referidas Orientaciones se indica que "*las medidas técnicas y organizativas que se adopten han de estar dirigidas específicamente a minimizar los riesgos identificados para los derechos y libertades de las potenciales brechas de datos personales. Esto implica que el responsable ha de evaluar los riesgos que pueden aparecer, diseñar medidas orientadas a minimizar su probabilidad e impacto, y determinar en qué grado dichas medidas están gestionando apropiadamente los riesgos concretos en un proceso dinámico*"

Y se añade que "*Las medidas apropiadas han de seleccionarse e implementarse desde el diseño de los tratamientos con el objeto de que todos los contextos de riesgo para los derechos y libertades sean considerados. Hay que tener en cuenta que algunas medidas serán más eficaces para evitar o mitigar el impacto directo sobre los individuos y otras medidas lo serán principalmente sobre el impacto social para los derechos fundamentales. Es necesario aplicar un alto nivel de protección de datos por defecto (…)*"

No se discute que una brecha de datos personales se pueda producir, por ello dentro de la gestión del riesgo de una determinada organización, precisamente porque se puede llegar a producir una brecha, debe encontrarse evaluado dicho escenario como parte indisoluble de la gestión del riesgo a los efectos de (i) adoptar todo tipo de medidas técnicas y organizativas apropiadas para evitar que se materialice y (ii) determinar medidas a posteriori para minimizar los daños. Sobre este particular las citadas Orientaciones explican que "*ante los posibles escenarios de materialización de distintos tipos de brechas hay que encontrar respuesta, al menos, a las siguientes preguntas desde el diseño del tratamiento y previamente a su implementación:*

• *Qué impacto personal y social puede tener una brecha de datos personales si se materializa.*

• *Qué medidas de protección de datos deberían estar implementadas a priori para minimizar el impacto personal y social que pudiera producir una brecha materializada.*

• *Qué medidas de respuesta deben estar previstas y deben ejecutarse a posteriori, una vez producida la brecha, para minimizar el impacto personal y social*".

Por lo tanto, su gestión no puede estar basada exclusivamente en el ámbito de la ciberseguridad, sino que tiene que englobar todos los ámbitos en los que se desarrolle el tratamiento, puesto que, si no, la gestión del riesgo no sería completa, y, por tanto, sería inútil. Para ello resulta imprescindible la adopción de medidas específicas para la protección de datos desde el diseño y por defecto, y además medidas para una gestión eficaz de las consecuencias de la brecha orientada a proteger los derechos fundamentales de las personas físicas.

Como se ha señalado, hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar el principio de confidencialidad.

En este sentido, I-DE no ha acreditado que haya cumplido con lo establecido en el RGPD, puesto que no se ha acreditado que, de conformidad con todo lo anterior, haya evaluado esos riesgos y aplicado medidas técnicas y organizativas apropiadas dirigidas a aplicar de forma efectiva los principios de protección de datos, entre ellas medidas dirigidas a garantizar el principio de confidencialidad. Y junto a ello se ha de resaltar que en este caso se ha materializado la quiebra del principio de confidencialidad

A mayor abundamiento, y aparte de lo anterior, ni siquiera en el análisis de los riesgos para adoptar las medidas de seguridad del artículo 32 se han indicado cuáles son las medidas a adoptar para paliar ese riesgo "medio" que indica que tiene la actividad de tratamiento afectada por la brecha, tal y como se le indica posteriormente de forma más extensa y pormenorizada en la respuesta a la alegación Cuarta del presente Fundamento de Derecho.

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 I-DE, lo que no supone una responsabilidad objetiva, pues I-DE no fue diligente al no garantizar, de esta forma, una seguridad adecuada mediante la aplicación de las medidas técnicas y organizativas apropiadas, no sólo de seguridad, sino de todo tipo.

En cuanto a lo señalado por I-DE relativo a que esta AEPD no ha acreditado de ninguna forma la materialización del riesgo que supone la pérdida de confidencialidad para las personas afectadas, que ningún cliente de I-DE ha visto afectados sus derechos como consecuencia de la brecha de seguridad acaecida, lo cual entiende que no permite considerar infringido un principio e imponer como consecuencia de dicha supuesta infracción la multa de dos millones de euros sobre la base de una mera potencialidad o la consideración de que se podría producir un alto riesgo de fraude, en modo alguno acreditado.

Frente a ello, y tal y como ya se le indicó en la Propuesta de Resolución, lo que se le imputa a I-DE es la vulneración del principio de confidencialidad pues consta que, tras sufrir un ataque informático contra la web GEA, se produjo un acceso ilegítimo a datos personales y la extracción de los mismos por un tercero no autorizado, lo que supuso la pérdida de confidencialidad y de control de numerosos datos personales (nombre y apellidos, DNI, dirección postal, fax, e-mail, teléfono, código cliente) y que afectó a 1.350.000 clientes de I-DE. Por tanto, el riesgo sí se materializó, la pérdida de confidencialidad y la pérdida de control sobre los datos. Lo que se garantiza es la confidencialidad a fin de evitar los graves daños que puede producir su quiebra, pues supone un riesgo alto para los interesados, en caso de vulnerarse la confidencialidad, de un uso fraudulento de los datos: suplantación de la identidad para la contratación en línea, phishing, fraude financiero, etc. La pérdida de confidencialidad ya se ha producido en este caso al haberse producido el acceso y la exfiltración, con lo cual no es ya que exista “probabilidad” de riesgo, sino concreción de este riesgo causando un daño por sí mismo. Ello supone el incumplimiento del deber de garantizar la confidencialidad de los datos personales, pues como se ha indicado, el artículo 5.1.f) señala que deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito.

Asimismo, en cuanto a que ninguno de sus clientes se ha visto afectados en ninguno de sus derechos como consecuencia de la brecha de seguridad, olvida I-DE que la propia pérdida de confidencialidad sufrida supone en sí misma que se vea afectado el núcleo del derecho fundamental a la protección de datos, que no es otro que la de disponer del control de los datos personales.

En cuanto a que se señaló el alto riesgo de que esos datos, en manos de ciberdelincuente/s, se usaran de forma fraudulenta, ello se indicó para expresar lo que supone la pérdida de confidencialidad, pero no es necesario en modo alguno, para entender infringido el artículo 5.1.f), que dichos riesgos de uso fraudulento se materialicen, porque lo que se ha materializado con la brecha es la pérdida de confidencialidad de los datos personales tratados por I-DE, que es lo que se le imputa exclusivamente.

Por lo expuesto, se desestima la alegación.

SÉPTIMA: Sobre la vulneración del principio de proporcionalidad en detrimento de los derechos de I-DE

Llama la atención I-DE que se han aplicado las mismas circunstancias agravantes en relación con las dos infracciones imputadas, lo que entiende que evidencia hasta qué punto la conexión entre ambas en total, procediendo la aplicación de lo invocado en las alegaciones Segunda y Tercera (vulneración del principio non bis in ídem y existencia de concurso medial)

A este respecto, ya se le indicó, en relación con la aplicación de idénticos agravantes en ambas infracciones, que las circunstancias previstas en el art. 83.2 del RGPD y las dispuestas en el art. 76.2 de la LOPDGDD son las únicas que se pueden aplicar por la AEPD para cualquier infracción.

Lo determinante en este caso no es que coincidan en su uso, sino la fundamentación que se establezca para su consideración.

Asimismo, alega I-DE la Improcedente aplicación del artículo 83.2.a) del RGPD, llamando la atención I-DE sobre el hecho de que se haya considerado que procede agravar la sanción impuesta por el hecho de que se haya producido una pérdida de confidencialidad de los datos personales, tanto en relación con el artículo 32 como con el artículo 5.1.f)

Así, sostiene I-DE que, en relación con la infracción del artículo 32, conforme al concepto tradicional de seguridad en los sistemas, la misma tiene por objeto la garantía de la integridad, confidencialidad y disponibilidad de la información, por lo que, si la AEPD considera que el hecho de que se produzca una brecha de confidencialidad agravaría la conducta consistente en la supuesta ausencia de tales medidas de seguridad, toda imputación por la supuesta infracción del artículo 32, resultará agravada por la AEPD, lo que conllevaría la inclusión en el catálogo de infracciones de una suerte de tipo agravado por su propia naturaleza, lo que sin embargo no aparece recogido en el RGPD ni en la LOPDGDD.

A este respecto, procede señalar, en contra de lo argumentado, que la vulneración de la confidencialidad no resulta necesaria o imprescindible en la comisión de la infracción del artículo 32, pues tal y como ya se ha indicado anteriormente, se puede vulnerar el citado artículo 32 por ausencia de medidas de seguridad apropiadas o por ineficiencia en su utilización o implantación, sin que necesariamente se haya producido una brecha de datos personales. Otra cosa distinta es que se ponga en evidencia la infracción del artículo 32 como consecuencia de la materialización de una violación de la seguridad de los datos personales que, por su propia definición, supone "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*" (apartado 12 de artículo 4 del RGPD)

Por tanto, en el presente caso, existía una vulnerabilidad en un aplicativo de I-DE, además de otras deficiencias como en la política de contraseñas y en los límites existentes en el acceso a la aplicación desde IPs sospechosas y no necesarias para el desarrollo del negocio, lo que puso de manifiesto que I-DE no estaba aplicando medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de sus tratamientos (no olvidar que se trata de un aplicativo web, es decir, con acceso desde internet), lo cual supone en sí mismo una vulneración del artículo 32. Si además dichas deficiencias han permitido o facilitado, como es el caso, que se haya producido una brecha de datos personales (en este caso, brecha de confidencialidad), no existe óbice alguno para considerar dicha violación como una circunstancia agravante del artículo 83.2.a) , el cual permite tener en cuenta la "naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido" (el subrayado es nuestro).

En cuanto a la aplicación del agravante del artículo 83.2.a) por vulneración del artículo 5.1.f), si bien es cierto que la vulneración de la confidencialidad no resulta adecuada como circunstancia a tener en cuenta para agravar la infracción por cuanto se

encuentra subsumida en el propio tipo infractor, también lo es que dicho precepto, el 83.2.a) del RGPD se ha aplicado como agravante teniendo en cuenta, además, el número de interesados afectados, que son muy numerosos, que asciende a más de un millón de personas (1.350.000), así como que fueron sustraídos numerosos datos personales (nombre y apellidos, DNI, dirección postal, e-mail, número de teléfono, código cliente), por lo que procede seguir teniendo en cuenta estas circunstancias como agravantes, por lo que sigue siendo aplicable el artículo 83.2.a) del RGPD.

En cuanto a que I-DE entiende que en relación a esta agravante se pretenden tener en cuenta unos supuestos daños y perjuicios sufridos, los cuales no han sido acreditados por la AEPD, se significa que lo que se tiene en cuenta en dicha agravante es el daño y riesgo que supone en sí mismo a pérdida de confidencialidad, que conlleva una total pérdida de control sobre los propios datos personales y el alto riesgo que conlleva de que se usen de forma fraudulenta, pues han sido sustraídos por un ciberdelincuente.

Por otro lado, aduce I-DE que no se le puede aplicar la agravante del artículo 83.2.b) del RGPD relativa a la existencia de negligencia ya que, en la Sentencia del Tribunal de Justicia Europeo, de 5 de diciembre de 2023 (asunto C-807/21), se declara que:

> "*75 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."*

De ello deduce I-DE que si es necesaria esa intencionalidad o negligencia para que pueda considerarse cometida la infracción, difícilmente puede considerarse que la forma más grave de culpabilidad exigible puede actuar como circunstancia agravante, y menos aún sobre un criterio subjetivo, como es el volumen de I-DE.

Frente a ello, procede señalar que una cosa es que, para poder imputar una infracción administrativa sea necesario la existencia de intención o negligencia y otra, que no pueda utilizarse como agravante la existencia de una negligencia especialmente puesta de relieve, por las circunstancias del caso. Lo opuesto sería contrario al propio artículo 83.2.b) que establece que "*Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

> *b) la intencionalidad o negligencia en la infracción"*

Así, en cualquier infracción de la normativa en materia de protección de datos ha de concurrir la existencia de intencionalidad o de negligencia. Y ello tanto a un responsable de tratamiento persona física, como persona jurídica, ya sea una pequeña empresa con poca vinculación con el tratamiento de datos personales, ya sea una gran empresa, una multinacional, etc, y con tratamientos de datos personales de forma continua y a gran escala, por ejemplo.

Por tanto, una vez determinado que, como premisa, concurre este elemento subjetivo culpabilístico de base, ello no obsta que se pueda considerar la agravante de intencionalidad o de negligencia indicada por considerar que, de conformidad con las

circunstancias concretas del caso, se considere un diferente grado de intencionalidad o de negligencia en el actuar del sujeto infractor. Así, de conformidad con las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, señala lo siguiente:

"4.2.2 — Carácter intencional o negligente de la infracción

55. En sus orientaciones anteriores el CEPD declaró que «en general, la intención incluye tanto el conocimiento como la voluntad en relación con las características de un delito, mientras que «no intencional» significa que no hubo intención de causar la infracción, aunque el responsable/encargado del tratamiento incumplió el deber de cuidado exigido por la ley.

Ejemplo 4 — Ilustraciones de intención y negligencia (del WP 253)

«Las circunstancias indicativas de infracciones intencionales pueden ser un tratamiento ilícito autorizado explícitamente por la alta jerarquía de la dirección del responsable del tratamiento, o a pesar del asesoramiento del delegado de protección de datos o incumpliendo las políticas existentes, por ejemplo, la obtención y el tratamiento de datos sobre los empleados de un competidor con la intención de desacreditar a ese competidor en el mercado. Otros ejemplos aquí pueden ser:

> *- la modificación de los datos personales para dar una impresión (positiva) engañosa sobre si se han cumplido los objetivos; lo hemos visto en el contexto de los objetivos para los tiempos de espera hospitalarios*
>
> *- el comercio de datos personales con fines comerciales, es decir, la venta de datos como «optados» sin comprobar o ignorar las opiniones de los interesados sobre cómo deben utilizarse sus datos*

Otras circunstancias, como la falta de lectura y cumplimiento de las políticas existentes, el error humano, la falta de comprobación de los datos personales en la información publicada, la falta de aplicación de actualizaciones técnicas en el momento oportuno, la falta de adopción de políticas (en lugar de simplemente la falta de aplicación) pueden ser indicativos de negligencia»;

56. *El carácter doloso o negligente de la infracción [artículo 83, apartado 2, letra b), del RGPD] debe evaluarse teniendo en cuenta los elementos objetivos de conducta obtenidos de los hechos del asunto. El CEPD destacó que en general se admite que las infracciones intencionales, «demostrar el desprecio por las disposiciones de la ley, son más graves que las no intencionales» En caso de infracción intencionada, es probable que la autoridad de control atribuya más peso a este factor. Dependiendo de las circunstancias del caso, la autoridad de control también puede atribuir peso al grado de negligencia. En el mejor de los casos, la negligencia podría considerarse neutral*." (el subrayado es nuestro)

En el presente caso, se apreció la agravante de negligencia por cuanto la vulnerabilidad detectada podría haberse evitado, siendo además una vulnerabilidad identificable en las evaluaciones de seguridad. Asimismo, en relación con la infracción

del artículo 5.1.f) del RGPD, se apreció también como agravante la negligencia mostrada por I-DE por cuanto, como se ha señalado, por sus circunstancias subjetivas y por el elevado número de clientes que tiene le es exigible un mayor grado de profesionalidad y de diligencia en el deber de garantizar la confidencialidad de los datos personales de sus numerosos clientes.

En cuanto a la consideración del tamaño de I-DE como agravante, procede señalar que no se puede exigir el mismo nivel de diligencia a una empresa como I-DE, que la exigible a una persona física o a un pequeño comercio, por ejemplo. Ello supone que se le exige un nivel de diligencia mayor por cuanto el nivel de profesionalidad es mayor.

Procede recordar de nuevo, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las previsiones legales al respecto*".

Por último, en contra de lo manifestado por I-DE, la consideración de esta agravante de negligencia en ningún momento ha supuesto que se haya incrementado el límite máximo de la sanción a imponer, pues los límites máximos se encuentran establecidos en los apartados 4 y 5 del artículo 83 del RGPD, los cuales permiten imponer una sanción, respectivamente de 10.000.000 de euros o el 2% del volumen de negocio total anual global y de 20.000.000 de euros o el 4% del volumen de negocio total anual global. Por tanto, en ningún momento se ha establecido el importe máximo de la sanción que podría imponerse como consecuencia de la aplicación de las agravantes tal y como indica I-DE.

En cuanto a la circunstancia agravante recogida en el artículo 76.2.b de la LOPDGDD, señala I-DE que se le está agravando su conducta por el mero hecho de pertenecer a un sector de actividad concreto. A este respecto, se significa que en dicho precepto no se tiene en consideración la actividad concreta a la que se dedica I-DE (distribuidora de energía), sino su vinculación con la realización de tratamientos de datos personales, ya que realiza tratamientos masivos y a gran escala (de 21 millones de clientes), a través de aplicaciones informáticas y aplicativos webs y de forma continua.

En este sentido, el legislador español ha considerado incluir en el artículo 76 de la LOPDGDD que: "*2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:*
(…)
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales."

Esta Agencia simplemente toma en consideración esa circunstancia, prevista por el legislador, a la hora de decidir la imposición de la multa administrativa.

Por último, alega I-DE la ruptura del principio de igualdad de trato si se tiene en consideración los precedentes de esta Agencia. Así, señala el procedimiento PS/000179/2020 en el que indica que se impuso una sanción menor a pesar de entender que las circunstancias fueron más graves, pero que, sobre todo, en dicho expediente no se impuso sanción alguna por vulneración del artículo 5.1.f) del RGPD, pese a ser manifiesta la existencia de una brecha de confidencialidad de los datos, habiendo la AEPD por tanto modificado su criterio, pues al convertir ahora lo que se consideraba una infracción del artículo 32 del RGPD en dos infracciones, al hacer ahora referencia al 5.1.f) del RGPD, y multiplicar considerablemente el importe total de la infracción, supone una flagrante quiebra del principio de igualdad, de seguridad jurídica y fe pública. Asimismo, señala que ello va también en contra de la doctrina de los actos propios.

Frente a ello, tal y como ya se señaló en la Propuesta de Resolución, las circunstancias y los hechos del procedimiento PS/000179/2020 no son iguales ni equiparables, así como que no cabe igualdad en la ilegalidad, por lo que no cabe intentar equiparar sanciones ante hechos y circunstancias diferentes. Por tanto, procede remitirse a lo respondido frente a esta misma alegación y que aparece transcrito en su totalidad en el apartado Sexto del Fundamento de Derecho IV de la presente Resolución.

En cuanto a lo que sostiene I-DE relativo a que se ha vulnerado el principio de igualdad también en el hecho de que en el PS/000179/2020 únicamente se sancionó por una infracción del artículo 32 y no se consideró infracción del artículo 5.1.f) del RGPD, habiendo existido también una brecha de confidencialidad, y que ello además va contra la doctrina de los actos propios, se significa que I-DE únicamente ha seleccionado y trae a colación este expediente para defender un supuesto trato desigual pero que, sin embargo, obvia los numerosos procedimientos sancionadores existentes con anterioridad al presente en el que, tras producirse una brecha de confidencialidad, se ha sancionado por haberse infringido ambos preceptos. A modo de ejemplo y sin carácter exhaustivo, pues existen más, procede indicar los siguientes: PS/00444/2021, PS/00420/2021, PS/00528/2021, PS/00099/2022, PS/00113/2022, PS/00164/2022, PS/00419/2022, PS/00168/2022.

Por último, en cuanto al procedimiento PS/0002/2023 en el cual se han impuesto también dos sanciones por infringir tanto el artículo 32 y el 5.1.f) del RGPD y que por referirse también a una empresa del sector eléctrico, trae a colación I-DE para hacer una comparativa, porque allí se impuso, en la suma total de las dos sanciones por estas dos infracciones, un importe que sólo supera en 500.000 euros a las impuestas a I-DE, a pesar de que hubo afectados perjudicados, se significa de nuevo que los hechos y las circunstancias son diferentes y que, por ello, se impuso una multa diferente (en este caso superior), además de otras multas por otras infracciones distintas que se consideraron.

En este sentido, de nuevo se recuerda 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. En este sentido, debe recordarse que el artículo 83, en su apartado 2 establece que "*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual…"* (el subrayado es nuestro)

Por tanto, hay que atender a las circunstancias de cada caso individual, no existiendo dos expedientes iguales y, por tanto, con resultados iguales.

Como consideración general y final, procede señalar que ninguna de las sanciones aplicadas vulnera el principio de proporcionalidad. Así, debe recordarse que los artículos 83.4 y 83.5 del RGPD, donde se encuentran tipificadas respectivamente la infracción del artículo 32 y la del artículo 5.1.f), establecen unos límites en las cuantías de las multas que se pueden imponer muy alejados de las que finalmente se han establecido.

Así, el artículo 83.4 del citado Reglamento, establece que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. A este respecto, de conformidad con la entidad Axesor, el volumen de negocios para 2022 de I-DE fue de ******CANTIDAD.2*** de euros, lo que hubiera permitido imponer una sanción de hasta ******CANTIDAD.3*** de euros, por la infracción del artículo 32.

Por su parte, el artículo 83.5 del RGPD establece que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. A este respecto, de conformidad con el volumen de negocios indicado, hubiera permitido imponer una sanción de hasta ******CANTIDAD.4*** de euros, por la infracción del artículo 5.1.f).

Por tanto, teniendo en cuenta lo anterior, así como la negligencia de I-DE al tener un aplicativo web con la vulnerabilidad detectada, con una política de contraseñas débil y con permisos de accesos desde IPs sospechosas y no necesarias para el desarrollo de su actividad empresarial (y mucho menos para el objetivo del aplicativo en cuestión), desde el que se accede a datos personales de sus clientes y teniendo en cuenta el elevado número de personas afectadas cuyos datos personales fueron exfiltrados por un ciberdelincuente, lo cual supone una pérdida de control sobre los datos personales de forma irremediable, con el riesgo que ello supone, no puede decirse que las sanciones finalmente impuestas vulneren el principio de proporcionalidad, teniendo en cuenta que "*Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias*" (el subrayado es nuestro)

VI

Integridad y confidencialidad

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

"*1. Los datos personales serán:*
(…)

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

El principio de integridad y confidencialidad de los datos exige una garantía de seguridad en la aplicación de medidas técnicas u organizativas que eviten la alteración de los datos personales, su pérdida, tratamiento o acceso no autorizado o ilícito. No es posible la existencia de este derecho fundamental si no se garantizan la confidencialidad, la integridad y la disponibilidad de los mismos.

De ahí que la integridad y la confidencialidad de los datos personales se consideren esenciales para evitar que los interesados sufran efectos negativos. Por ello, deben tratarse de un modo que se garantice una integridad y confidencialidad adecuadas de los datos personales, especialmente para impedir el acceso tratamiento o uso no autorizados de dichos datos.

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

A este respecto, debe recordarse que la confidencialidad de los datos personales se regula en el artículo 5 del RGPD siendo, por tanto, uno de los principios relativos al tratamiento. Los principios relativos al tratamiento son, por un lado, el punto de partida y la cláusula de cierre del ordenamiento jurídico de protección de datos, constituyendo verdaderas reglas informadoras del sistema con una intensa fuerza expansiva; por otro lado, al tener un alto nivel de concreción, son normas de obligado cumplimiento susceptibles de ser infringidas.

El artículo 5.1.f) del RGPD establece una obligación clara de cumplimiento consistente en impedir tratamientos no autorizados o ilícitos implementando medidas de todo tipo adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos. En consecuencia, los responsables del tratamiento deben estar en disposición de garantizar la confidencialidad de los datos personales para impedir que un tercero acceda a datos que no son de su titularidad, pues precisamente les compete tratar los datos personales conforme al RGPD y LOPDGDD. Por esta razón, es una actividad en donde la diligencia prestada por éstos es fundamental para evitar este tipo de accesos no autorizados.

En el presente caso, se ha vulnerado el principio de confidencialidad pues consta que tras sufrir un ataque informático contra la web de gestión de acometidas de I-DE (GEA), aprovechando una vulnerabilidad de la misma, se produjo un acceso ilegítimo a datos personales y la extracción de los mismos, lo que supuso la pérdida de confidencialidad y de control de numerosos datos personales (nombre y apellidos, DNI, dirección postal, fax, e-mail, teléfono, código cliente) y que afectó, entre otros, a 1.350.000 clientes de I-DE. Ello supone el incumplimiento del deber de garantizar la confidencialidad de los datos personales, pues como se ha indicado, el artículo 5.1f) señala que *deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito.*

Por tanto, el riesgo de pérdida de confidencialidad se ha materializado, habiendo sido usurpados por un ciberdelincuente, lo que supone que pueden ser utilizados para usos no conocidos (vendidos, comunicados, publicados, etc.), todo ello sin consentimiento de sus titulares, conllevando una pérdida total y absoluta de control sobre los mismos. Además, supone también un riesgo muy alto de uso fraudulento de los mismos (usurpación de identidad, fraude, pérdidas financieras, etc) o de que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para sus titulares. Debe tenerse en cuenta además que la mayoría de los datos personales filtrados son datos que no pueden ser modificados o cambiados por otros (nombre, apellidos, DNI, domicilio…)

Esta pérdida de control sobre los propios datos personales se traduce en una vulneración del derecho fundamental a la protección de datos reconocido en el artículo 18 de la Constitución Española pues tal y como ha indicado el Tribunal Constitucional (Sentencia 292/2000, de 30 de noviembre de 2000) "el derecho fundamental a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado (…) El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos"

Por todo lo expuesto y de conformidad con las evidencias de las que se dispone en este momento de propuesta de resolución, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a I-DE, por vulneración del artículo 5.1.f) del RGPD.

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

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

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del*

volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

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

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

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

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

VIII

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

De conformidad con las evidencias de que se dispone procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- Artículo 83.2.a) RGPD: Naturaleza, gravedad y duración de la infracción.

> -Número de interesados afectados: son muy numerosos los afectados, pues asciende a más de un millón de clientes de I-DE (1.350.000).
>
> -Nivel de los daños y perjuicios sufridos: Alto. Fueron sustraídos numerosos datos personales (nombre y apellidos, DNI, dirección postal, e-mail, número de teléfono, código cliente) y de un número muy considerable de clientes de I-DE (1.350.000) perdiendo, por tanto, todo control sobre los mismos, vaciando así de contenido el derecho fundamental a la protección de datos personales que, como indica el Tribunal Constitucional en la Sentencia anteriormente reseñada, persigue garantizar a la persona un poder de control y disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

- Artículo 83.2.b) RGPD. Intencionalidad o negligencia en la infracción: se aprecia la existencia de negligencia en el cumplimiento y observancia de las medidas técnicas y organizativas para garantizar la seguridad necesaria para la protección de los datos personales, concretamente para garantizar la confidencialidad de estos. A este

respecto, debe recordarse que I-DE es una gran empresa, que realiza tratamientos a gran escala, afectando sus tratamientos a numerosas personas físicas (21 millones de personas) por lo que se le exige un nivel de diligencia mayor.

Procede recordar, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las previsiones legales al respecto*".

Como atenuantes:

- Artículo 83.2.c) RGPD. Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados: Positivas. En cuanto fue consciente del ataque, reaccionó lo más rápido posible y se procedieron a tomar medidas dirigidas a repeler el mismo y para evitar su repetición (suspensión del aplicativo web; bloqueo de IPs sospechosas, desconexiones, etc) y activación inmediata de sus protocolos internos correspondientes, lo que pudo haber evitado un impacto mucho más grave.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "Sanciones y medidas correctivas" de la LOPDGDD:

Como agravantes:

- Artículo 76.2.b) LOPDGDD. Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal: El desarrollo de la actividad empresarial que desempeña I-DE suponer un tratamiento continuo y a gran escala de datos personales, pues, según manifiesta, trata datos de 21 millones de personas. Por tanto, se trata de una empresa grande habituada al tratamiento de datos personales.

De conformidad con las evidencias de que se dispone, teniendo en cuenta las circunstancias del caso y los criterios que establece el artículo 83.2 del RGPD con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, se establece una sanción de 2.500.000 € (dos millones y medio de euros).

IX

Artículo 32 del RGPD

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

"*1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y*

organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

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

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

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

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

El artículo 32 no establece medidas de seguridad estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

En consonancia con estas previsiones, el Considerando 75 del RGPD establece: Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión

o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados. (el subrayado es nuestro)

Asimismo, el Considerando 83 del RGPD establece: A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales. (el subrayado es nuestro)

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

La seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos personales si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD citado, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Por tanto, I-DE, a la hora de evaluar los riesgos y determinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, está obligada a tener en cuenta la concreta actividad que supone su negocio, que conlleva tratar datos personales de forma continua y a gran escala (numerosos datos a recoger, procesar, almacenar…); la tipología de datos tratados: identificativos, de

contacto, los relativos al suministro y al consumo de electricidad, cuentas corrientes, etc); el contexto: utilización de un aplicativo web en internet, es decir, en un entorno no aislado, lo que conlleva riesgos derivados de la propia interconectividad que supone la red, los cuales deben atenderse de forma especializada.

Por ello, derivado de la actividad a la que se dedica, I-DE está obligada a realizar de forma muy especializada un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las personas.

En el presente caso, como se ha señalado anteriormente, I-DE sufrió un ciberataque a su aplicativo web GEA, causando una brecha de seguridad consistente en una brecha de confidencialidad al producirse un acceso a datos personales de sus clientes, contenidos en la base de datos del Grupo y una exfiltración ilícita de los mismos.

La aplicación GEA es una aplicación web de I-DE que se utiliza para la gestión de acometidas eléctricas. Está publicada en Internet para su acceso por parte de los usuarios (clientes, instaladores, etc) implicados en el proceso de gestión de esos expedientes de acometida.

(…)

Todo lo expuesto demuestra que I-DE no fue lo suficientemente diligente a la hora de implantar medidas de seguridad apropiadas para impedir que se produjeran incidentes de seguridad como el que tuvo lugar en el presente caso, es decir, no aplicó medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de sus tratamientos de datos personales. Asimismo, tampoco se aprecia la diligencia necesaria en el proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. (artículo 32.1)

Por tanto, de conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable a I-DE, por vulneración del artículo 32 del RGPD.

X

Tipificación de la infracción del artículo 32 del RGPD

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

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

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

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

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

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

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

XI
Sanción por la infracción del artículo 32 del RGPD

De conformidad con las evidencias de que se dispone procede graduar la sanción a imponer, de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- Artículo 83.2.a) RGPD: Naturaleza, gravedad y duración de la infracción.

-Se considera que la naturaleza de la infracción es grave puesto que ha acarreado una pérdida de confidencialidad y, por tanto, de disposición y control irremediable sobre los datos personales.

-Número de interesados afectados: son muy numerosos los afectados, pues asciende a 1.350.000

-Nivel de los daños y perjuicios sufridos: Alto. Fueron sustraídos numerosos datos personales (nombre y apellidos, DNI, dirección postal, e-mail, número de teléfono, código cliente) y de un número muy considerable de clientes de I-DE (1.350.000) perdiendo, por tanto, todo control sobre los mismos, vaciando así de contenido el derecho fundamental a la protección de datos personales que, como indica el Tribunal Constitucional en la Sentencia anteriormente reseñada, persigue garantizar a la persona un poder de control y disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

- Artículo 83.2.b) RGPD. Intencionalidad o negligencia en la infracción: se aprecia la existencia de negligencia en el cumplimiento y observancia de las medidas técnicas y

organizativas para garantizar una seguridad adecuada para la protección de los datos personales, concretamente para garantizar la confidencialidad de estos. La vulnerabilidad detectada podría haberse evitado, siendo además una vulnerabilidad identificable en las evaluaciones de seguridad.

A este respecto, debe recordarse que I-DE es una gran empresa, que realiza tratamientos a gran escala, afectando sus tratamientos a numerosas personas físicas (21 millones de personas) por lo que se le exige un nivel de diligencia mayor y medidas de seguridad adecuadas para garantizar la confidencialidad de los datos personales que trata.

Procede recordar, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las previsiones legales al respecto*".

Como atenuantes:

- Artículo 83.2.c) RGPD. Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados: Positivas. En cuanto fue consciente del ataque, el personal de I-DE reaccionó lo más rápido posible y procedió a tomar medidas dirigidas a repeler el mismo y para evitar su repetición (suspensión del aplicativo web; bloqueo de IP sospechosas, desconexiones, etc) y activación inmediata de sus protocolos internos correspondientes, lo que pudo haber evitado un impacto mucho más grave.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "Sanciones y medidas correctivas" de la LOPDGDD:

Como agravantes:

- Artículo 76.2.b) LOPDGDD. Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal: El desarrollo de la actividad empresarial que desempeña I-DE supone un tratamiento continuo y a gran escala de datos personales. Por tanto, se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite establecer una sanción de 1.000.000 € (un millón de euros).

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

PRIMERO: IMPONER a I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U., con NIF A95075578, por una infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD, una multa de 2.500.000 euros (DOS MILLONES QUINIENTOS MIL EUROS).

SEGUNDO: IMPONER a I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U., con NIF A95075578, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una multa de 1.000.000 (UN MILLÓN DE EUROS)

TERCERO: NOTIFICAR la presente resolución a I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U.

CUARTO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 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, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad 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 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente

recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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

938-16012024

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