- **Expediente N.º: EXP202307113**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.***, ***B.B.B., C.C.C., D.D.D., E.E.E., F.F.F., G.G.G.*** y ***H.H.H.,*** (en adelante, la parte reclamante) interpusieron reclamaciones ante la Agencia Española de Protección de Datos. Las reclamaciones se dirigen contra XFERA MÓVILES, S.A.U., con NIF A82528548 (en adelante, la parte reclamada o XFERA).

Los motivos en que basan sus reclamaciones son los siguientes:

Reclamación 1, fecha de entrada 2 de abril de 2023 y registro REGAGE23e00021932536, con los siguientes datos asociados:

- Reclamante: ***A.A.A.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" He *recibido correo del proveedor de telefonía indicando que terceras personas han accedido a datos personales con el objeto de suplantación de identidad, razón por la cual, quiero interponer demanda, ya que no han garantizado la seguridad e integridad de la información personal que se les ha suministrado.*"
- Aporta captura con correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 1 de abril de 2023 con información sobre un incidente de seguridad que afectó a sus datos personales.

Reclamación 2, fecha de entrada 8 de abril de 2023 y registro REGAGE23e00022985593, con los siguientes datos:

- Reclamante: ***B.B.B.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Brecha de seguridad en la base de datos de clientes de Yoigo; terceras personas se han hecho con datos personales míos, sin mi autorización, con el riesgo que conlleva. Dicha posible brecha se me informo ayer 07/04/2023 por correo electrónico y se me ha confirmado hoy día 8 de abril mediante llamada telefónica al número* ******TELÉFONO.2,*** *número que se me indicaba en el correo y que me han confirmado por Twitter, de Yoigo donde se me ha indicado que los datos sustraídos son, como mínimo, mi nombre, número de identificación, teléfono y número de cuenta bancaria*".
- Aporta captura de pantalla con la información recibida por parte de Yoigo comunicando el incidente de seguridad.

Reclamación 3, fecha de entrada 10 de abril de 2023 y registro REGAGE23e00023162950, con los siguientes datos:

- Reclamante: ***C.C.C.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *YOIGO remitió a sus clientes un correo electrónico informativo con fecha 6 de abril de 2023, a las 14:07 horas, en el que se nos comunicaba tales circunstancias (correo que adjunto al presente escrito), y que pude constatar al contactar con el servicio de atención al cliente de la operadora en la que confirman que mis datos se han visto afectados, desde el nombre y dirección, hasta el DNI o el número de la cuenta corriente.* "
- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 6 de abril de 2023 comunicando el incidente de seguridad y la afectación de sus datos personales."

Reclamación 4, con fecha de entrada 10 de abril de 2023 y registro REGAGE23e00023074494, con los siguientes datos:

- Reclamante: ***D.D.D.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *En el mes de marzo se me ha añadido un coste en la factura del teléfono de 1.99. Al contactar con Yoigo me dicen que no saben de donde procede y que lo único que saben es que se dado de alta en tienda física de Yoigo. Me dan un teléfono (*****TELÉFONO.1**) para que pueda aclarar importe. Es una empresa que protección de datos, pero yo no he contratado. Tampoco me dicen de donde ha salido el alta. Me informan que puedo enviar correo para dar de baja. (*****EMAIL.2)** para dar de baja una póliza que nunca he contratado. El importe no me lo devolverán. Días más tarde recibo mail de Yoigo donde especifica que 'debemos ponernos en contacto contigo para informarte que hemos experimentado un incidente, por el cual terceras personas ajanes a nuestra organización pueden haber accedido a algunos de tus datos personales...'*
- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 6 de abril de 2023 con la información sobre el incidente de seguridad y la afectación de datos personales."

Reclamación 5, con fecha de entrada 23 de abril de 2023 y registro REGAGE23e00025932054, con los siguientes datos asociados:

- Reclamante: ***E.E.E.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Me dirijo a ustedes con relación al robo de datos personales que ha sufrido mi compañía telefónica, XFERA MOVILES SAU, con nombre comercial YOIGO.A pesar de ser uno de sus clientes, no he recibido ninguna información sobre qué datos míos se han visto comprometidos. Por tanto, me gustaría hacer una reclamación por el tratamiento de mis datos personales. Solicito que se me informe qué datos míos se han visto comprometidos y cómo se han visto afectados, teniendo en cuenta que también se pueden haber visto*

comprometidos los datos de las líneas de las que soy titular siendo 3 líneas móviles y 1 línea fija. Además, solicito que se tomen las medidas necesarias para garantizar que esto no vuelva a suceder. Asimismo, considero que he sufrido daños y perjuicios como resultado de este incidente y solicito que se me indemnice adecuadamente por ello, teniendo en cuenta además como he indicado anteriormente que soy titular de 4 líneas telefónicas en la compañía y se pueden haber visto comprometida también información de las mismas. "

- Aporta:
  - Captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1***, en fecha 6 de abril de 2023, con la información sobre el incidente de seguridad y la afectación de datos personales.
  - Copia de DNI, copia del contrato con la compañía y factura de servicios.

Reclamación 6, con fecha de entrada 23 de abril de 2023 y registro REGAGE23e00026221929, con los siguientes datos asociados:

- Reclamante: ***F.F.F.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Debido al ciberataque sufrido por Yoigo a principios de marzo, me informan que mis datos PERSONALES podrían haber sido expuesto (nombre, apellidos, números de teléfono, DNI, CUENTA BANCARIA, etc.) a ciberdelincuentes. Debido a esto, desde hace 2-3 semanas he recibido phishing muy sofisticado, pero eso no es lo grave. Lo grave, es que mi cuenta bancaria corresponde a un banco vasco muy pequeño, y debido a que les han sustraído mis datos, los ciberdelincuentes saben perfectamente a que banco corresponde mi cuenta bancaria (por el IBAN). Por este motivo, el phishing que estoy recibiendo a todas horas, no solo es sofisticado, sino que está totalmente teledirigido a mi porque conocen todos los datos que arriba menciono. Estoy tremendamente afectado y con el temor de cualquier día caer en la trampa, porque he visto mucho phishing, pero este es muy sofisticado. Como cliente de Yoigo, me veo tremendamente perjudicado y gracias a a esta empresa, vivo con la angustia de caer en alguna trampa y perder mi patrimonio. La presente reclamación es debido a que Yoigo no ha hecho una correcta custodia de mis datos personales y esto me está provocando graves daños psicológicos por las razones antes expuestas. Es curioso, que, dentro de mi contrato, hay 3 líneas más, pero la única que recibe el phishing soy yo, porque soy el titular del contrato y de la cuenta bancaria. Es una evidencia, que este ataque no responde al azar.* "
- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 5 de abril de 2023 con la información sobre el incidente de seguridad y la afectación de datos personales.

Reclamación 7, con fecha de entrada 11 de mayo de 2023 y registro REGAGE23e00030222022, con los siguientes datos asociados:

- Reclamante: ***G.G.G.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *El día 2 de abril de 2023, recibo un mail de dicha empresa Yoigo que aporto como prueba documental adjunta al presente escrito, en virtud de la cual, se me pone en*

conocimiento de la existencia de un ciberataque en la citada empresa, lo que ha motivado que mis datos personales tanto propios como los de mi familia que figurasen almacenados pudieran haber quedado expuestos frente a terceros de forma indebida. Tras llamar al número de teléfono que figura en el mail no me facilitaron más información que la que ya consta en el mail aportado (no concretando qué datos en particular serían o si ha sido en grado de tentativa o efectivamente se ha consumado una intromisión indebida, y por supuesto tampoco admiten ninguna reparación o indemnización por ello al cliente). Desde dicha fecha vengo recibiendo mensajes fraudulentos como por ejemplo un mail manifestando que tengo un paquete esperando, o algunos SMS suplantando mi Banco manifestando que tengo un problema en mi cuenta, lo que claramente se infiere que se trata de mensajes fraudulentos o phishing. El perjuicio consistente en que puedan suplantarme o el temor a un potencial futuro uso indebido de sus datos personales, cuya existencia haya sido demostrada por el interesado, puede constituir un daño moral que genere derecho a indemnización "

- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 2 de abril de 2023 con la información sobre el incidente de seguridad y afectación de datos personales.

Reclamación 8, con fecha de entrada 30 de mayo de 2023 y registro REGAGE23e00034386550, con los siguientes datos asociados:

- Reclamante: ***H.H.H.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" Soy *cliente de Yoigo. En abril recibí un mail en el que se me comunicaba que TODOS los datos de los clientes habían sido filtrados. Solicité que me dijeran explícitamente qué datos. Este grupo ha infringido el RGPD y la LOPDGDD al no custodiar debidamente la información requerida para contratar sus servicios y desde ahora mi identidad puede ser manipulada para fines ilícitos y por tiempo indeterminado. Me gustaría acogerme al amparo de la AEPD ya que esta filtración supone una situación de vulnerabilidad personal crítica por las incorrectas medidas de seguridad tomadas por la empresa Yoigo-GRUPO MASMOVIL - XFERA MOVILES, S.A.U.* "
- Aporta:
    - Captura de pantalla del correo inicial recibido desde la dirección ******EMAIL.1*** en fecha 3 de abril de 2023 con información sobre el incidente de seguridad y afectación de datos personales.
    - Captura de pantalla de correo enviado por el reclamante a la dirección ******EMAIL.3*** solicitando información adicional sobre el incidente.
    - Captura de pantalla de correo de respuesta recibido desde la dirección ******EMAIL.3*** con el siguiente contenido:

      "*En relación con el incidente, le informamos que hemos detectado un acceso no autorizado a una de las aplicaciones que dan soporte a nuestro canal presencial que permite la visualización de ciertos datos, como datos identificativos, de contacto, información de los servicios contratados con nosotros y el IBAN.*

Como indicábamos en la comunicación, es posible que estos datos sean utilizados para intentar usurpar su personalidad, principalmente ante nosotros, si bien hemos modificado nuestras políticas para evitar dicha circunstancia. También le informamos que solo con la información accedida no debería ser posible, por ejemplo, contratar ningún servicio (puesto que requiere de un mandato SEPA) ni acceder a su cuenta bancaria.
En todo caso, le recomendamos que tenga cuidado con correos electrónicos, SMS o llamadas que pueda recibir de remitentes desconocidos o que no se identifiquen claramente, en especial si le solicitan códigos, claves de acceso o datos de tarjeta de crédito.
En caso de que detecte cualquier actividad sospechosa, le recomendamos que se ponga en contacto con su entidad bancaria y denuncie los hechos a la policía. También puede ponerse en contacto con el Instituto Nacional de Ciberseguridad (INCIBE) en el número 017 o consultar su sitio web ******URL.1.***
Esperamos haber resuelto sus cuestiones, en cualquier caso, estamos a su disposición"

SEGUNDO: Previamente a estas reclamaciones, el 31 de marzo de 2023, XFERA se puso en contacto con la AEPD para realizar la notificación de la quiebra de seguridad de datos personales relacionada con las reclamaciones anteriores. Con fecha 28 de abril de 2023 y registro de entrada REGAGE23e00027432375, XFERA amplió la información sobre la quiebra. De su contenido se extrae la siguiente información relevante

- *Los datos no estaban cifrados, anonimizados o protegidos de forma ininteligible.*
- *Descripción de la brecha:* "***(…)"***
- Número aproximado de personas físicas sobre las que se realizan operaciones de tratamiento referidas al tratamiento sobre el que se ha producido la brecha de datos personales: ******CANTIDAD.1***
- Afectados ******CANTIDAD.2.***
- Fecha de detección de la brecha: 28/03/2023
- Fecha de inicio de la brecha: 05/03/2023
- Fecha en la que se dio por resuelta la brecha: 03/04/2023
- Se comunicó a ******CANTIDAD.3***.
- Fecha en la que se informó: 10/04/2023

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de las reclamaciones a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, fue recibido en fecha 7 de junio de 2023, como consta en el certificado que obra en el expediente.

En fecha 6 de julio de 2023 y registros de entrada REGAGE23e00045313624 y REGAGE23e00045317575, se recibe en esta Agencia escrito de respuesta por parte de XFERA al traslado de las reclamaciones. Dichas reclamaciones fueron admitidas a trámite.

El análisis de la documentación aportada se detalla en el siguiente hecho cuarto.

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

En fecha 6 de julio y registro de entrada REGAGE23e00045313624, se recibe respuesta por parte de XFERA al traslado de las reclamaciones, de la documentación aportada se extrae la siguiente información relevante para la investigación:

En relación con el contexto cronológico proporcionan las siguientes afirmaciones:

- ***(…).***

Afirman que, al tenerse constancia del ataque, XFERA realizó de forma inmediata un primer análisis de riesgos para evaluar las consecuencias para las personas afectadas, adoptando una serie de decisiones y medidas para minimizar estas posibles consecuencias, este análisis fue actualizado posteriormente en fecha 7 de junio de 2023. Aportan documentación acreditativa, de su análisis se extrae el siguiente contenido relevante para la investigación:

- Se valora riesgo inherente repercutido por la brecha como *Muy Alto*, teniéndose en cuenta los siguientes factores de riesgo: "*usurpación de identidad, fraude y posibles pérdidas económicas significativa*s.
- Se incluyen las siguientes medidas de contención adoptadas para mitigar el riesgo:
  - ***(…)***

Se aporta copia del Registro de Actividades de Tratamiento (RAT) con información de la actividad afectada por la brecha y el análisis de riesgos para los derechos y libertades en este tratamiento, el documento aportado no incorpora firma ni fecha de creación, no obstante, en su contenido se menciona como fecha de realización del análisis: el mes de diciembre de 2022. Del análisis de este documento se extrae la siguiente información relevante:

- ***(…)***

En relación con la notificación y la comunicación de la brecha, afirman que notificaron ante esta Agencia inicialmente en fecha 31 de marzo de 2023 y de forma completa en

fecha 28 de abril de 2023. La comunicación a los afectados se inició a partir del 31 de marzo de 2023.

En relación con las medidas adoptadas por XFERA para que no se vuelva a producir un incidente similar, afirman:

- ***(…)***

De la respuesta proporcionada por XFERA se extrae también la siguiente afirmación relevante:

"***(…)".***

En la respuesta de XFERA se aporta la contestación individualizada que da la entidad a cada una de las reclamaciones que se adjuntaron en el traslado.

Teniendo en cuenta la información obtenida a raíz de las reclamaciones, de la respuesta al traslado y de la notificación de la brecha, se decide realizar nuevo requerimiento de información al responsable de tratamiento XFERA, en fecha 31 de octubre de 2023, marcado por la siguiente línea de investigación:

- Investigar los casos de uso del software afectado (VFR) y su afectación por la brecha.
- Solicitar acreditación de las medidas de autenticación del software VFR e investigar detalles de los trabajos realizados en los DNS que dieron lugar al posterior incidente de seguridad.
- Investigar los mecanismos de monitorización que existían implantados y solicitar acreditación de la detección del incidente por parte de la entidad.
- Solicitar acreditación de las medidas implantadas tras la brecha para reforzar la gestión de cambios en los DNS y resto de medidas reactivas desplegadas.
- Investigar los detalles de la tipología de datos afectada y el número final de personas físicas involucradas.
- Investigar las comunicaciones a las personas afectadas.
- Investigar el procedimiento interno implantado para gestionar brechas de seguridad.

En fecha 21 de noviembre de 2023 y registros de entrada REGAGE23e00079341750, REGAGE23e00079342044 y REGAGE23e00079342222 se recibe respuesta al requerimiento anterior por parte de XFERA, de su análisis se extrae la siguiente información relevante:

- En relación con la aplicación afectada afirman:

  "***(…)".***

- Por parte del inspector se analiza el documento proporcionado con la información sobre los casos de uso del software VFR, obteniéndose la siguiente información relevante:

  - El caso de uso afectado por la brecha es "*Búsqueda de datos de clientes*".

- Tiene como entrada para la búsqueda el *MSSISDN* y *N.º Documento* (*se afirma que en el momento de la brecha se pedía MSSISISDN o N.º de Documento*).
- Los datos visualizados como resultado de la búsqueda son:

"(…)"

Se aporta documento que acredita la implantación ***(…)***).

Con posterioridad se solicita información adicional en nuevo requerimiento de información sobre el tipo de trabajo realizado y los mecanismos de control que existieron.

- ***(…).***

- En relación con la acreditación de las medidas reactivas implantadas tras la brecha para reforzar la seguridad de los cambios en la infraestructura DNS y la monitorización del aplicativo VFR, afirman:

  - En relación con las medidas implantadas para reforzar la gestión de los DNS se aporta documento que acredita, a través de capturas de pantalla, ***(…).***
  - En cuanto a las medidas introducidas para reforzar la monitorización interna del aplicativo, se aporta documento con información sobre las reglas implantadas en el sistema de monitorización empleado por XFERA tras la brecha, ***(…)***.

- Se aporta copia de la denuncia presentada el 19 de abril de 2023 ante Policía, de su contenido se extrae para la presente investigación:

  *"****(…)".***

- En relación con la denuncia interpuesta ante la Policía proporcionan la siguiente afirmación:

  "***(…)***".

- En respuesta a nuestra solicitud para que se acredite el procedimiento de gestión de brechas implantado en la organización, aportan documento acreditativo con título "PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y BRECHAS DE SEGURIDAD" y fecha de creación 01 de julio de 2022, este documento incluye apartados con la siguiente información:

  - *El diagrama de flujo del proceso interno de gestión de brechas.*
  - *Sobre el proceso de identificación del incidente, notificación, registro, análisis, clasificación, escalado, recopilación de evidencias, respuesta, comunicación, cierre y archivo del incidente.*
  - *Responsabilidades en el proceso de gestión de incidentes.*

- Afirman que entre las medidas adoptadas tras la brecha se implantaron sistemas de vigilancia digital en búsqueda de cualquier dato de los clientes que pudiese estar siendo utilizado o vendido en foros fraudulentos, indicando que esta medida sigue en curso y afirman:

  "*Hemos de decir que no ha aparecido en este proceso de búsqueda ningún dato de los afectados por la brecha a la venta o publicado en ningún lugar de la Deep Web desde que aconteció la fuga hasta el día de la presente*".

- En relación con la comunicación de la brecha a los afectados, afirman que se comunicaron a ******CANTIDAD.3,*** el 99,80% de los casos. La comunicación se realizó por correo electrónico y envío de SMS para aquellos clientes que no disponían del dato email. Afirman: "*la brecha de seguridad fue objeto de noticia en medios de comunicación de índole nacional y se puso a disposición de todos los clientes un número de teléfono gratuito que estuvo operativo en el que podían solicitar información de su afectación o no en el incidente, este número fue el ***TELÉFONO.2*".

En fecha 12 de marzo de 2024 se realiza un nuevo requerimiento de información dirigido al responsable de tratamiento XFERA, marcado por la siguiente línea de investigación:

- Solicitar nuevamente aclaración sobre la filtración de las credenciales del usuario de la aplicación VFR.
- Solicitar aclaración de los trabajos que provocaron los cambios de DNS.
- Solicitar aclaración y acreditación de la medida reactiva implantada para mejorar la seguridad en la validación de cambios de los DNS.
- Solicitar aclaración y acreditación de las nuevas reglas de monitorización que se incluyeron en los sistemas para detectar y alertar de patrones anómalos.
- Solicitar aclaración del motivo por el que se permitían accesos al aplicativo VFR en horarios no habituales de tiendas y distribuidores.
- Solicitar aclaración de la medida reactiva implantada eliminación del IBAN como dato de autenticación.

En fecha 9 de abril de 2024 y registro de entrada REGAGE24e00026239512 se recibe respuesta al requerimiento anterior por parte de XFERA, de su contenido se extrae la siguiente información relevante para la investigación:

- Afirman que no se dispone de información adicional a la ya facilitada relativa a cómo se pudo comprometer las credenciales utilizadas por los atacantes.
- En relación con los procedimientos de validación que existían en la organización para garantizar la corrección de los trabajos realizados en cambios de DNS, afirman:

  "*(…)*".

  Por parte del inspector incluye nota aclaratoria del concepto "****CONCEPTO.1*", que consisten en la capacidad de gestionar y configurar la infraestructura de IT de la organización a través de código en lugar de hacerlo

manualmente, creándose archivos de configuración con los requisitos necesarios, facilitando la edición y distribución de las configuraciones. Un aspecto clave de la *IaC* es el control de versiones de los archivos, que debe tenerse en cuenta al igual que se hace con cualquier otro archivo de código fuente del software.

- En relación con la medida reactiva implantada tras la brecha para garantizar la seguridad en los cambios de DNS, afirman:

  "*Nos remitimos a la información facilitada a esta Agencia en noviembre de 2023 en lo relativo a la activación del control de cambios en los trabajos de modificación de configuración del DNS, donde figura la obligación de la necesaria doble validación de los trabajos sobre los DNS que anteriormente no se requería*".

Aportan captura de pantalla con nuevas evidencias de la implantación de la doble validación requerida (necesidad de aprobación por dos personas diferentes) para cualquier trabajo que se ejecute sobre cambios en DNS.

- En relación con la detección de la brecha y el software de monitorización existente afirman:

  "***(…)***".

Por parte del presente inspector se realiza búsqueda en internet para obtener información adicional sobre las herramientas mencionadas (******HERRAMIENTA.1 y ***HERRAMIENTA.2***), obteniéndose el siguiente texto de la web del producto (se crea diligencia y adjunta como objeto asociado al expediente):

"***(…)***".

- En relación con las reglas que existían en el sistema de monitorización antes de la brecha, afirman: "*En* ******SISTEMA.1*** *se establecía regla para la gestión del rendimiento y consumo*". Se aporta documento con captura de pantalla del servicio que se utilizaba (******SISTEMA.2***) con el conjunto de reglas incluidas, visualizándose únicamente el título de cada una de ellas: ***(…)***.

- En relación con las reglas que se incluyeron tras la brecha como medida reactiva afirman y acreditan documentalmente:

  "*Actualmente en el SIEM de* ******PLATAFORMA.1*** *se encuentran implementados los siguientes casos de uso relativos a reglas de detección de comportamientos anómalos personalizadas y automatización de acciones a través de* ******HERRAMIENTA.2****:*

  - ***(…)***".

- En respuesta a nuestra solicitud para que aclaren el motivo por el que se permitían accesos al aplicativo afectado (VFR) en horarios no habituales para tiendas y distribuidores, afirman:

"*(…)*".

- En respuesta a nuestra solicitud para que aporten información aclaratoria en relación con la eliminación del IBAN como dato de autenticación, afirman:

  "(…)".

- En respuesta a nuestra consulta para que aclaren si entre los datos filtrados existían copias de los DNI de clientes, afirman:

  "*(…)*".

CONCLUSIONES DE LAS ACTUACIONES PREVIAS DE INVESTIGACIÓN

1.- (…)

4.- En relación con la notificación de la brecha, en fecha 31 de marzo de 2023 se tiene constancia de la filtración de datos personales y se notifica a la AEPD este mismo día, completándose con una notificación adicional el 28 de abril de 2023. El mismo 31 de marzo de 2023 se inicia el proceso de comunicación a las personas afectadas, realizándose un total de ***CANTIDAD.3 comunicaciones vía email y SMS. La comunicación enviada informa sobre el ataque sufrido por la entidad, la filtración de algunos datos personales (no especifica cuales), las posibles consecuencias de la filtración, recomendaciones de medidas a adoptar por los afectados y datos de contacto para ofrecer más información.

5.- Ha quedado acreditado la existencia de análisis de riesgos para los derechos y libertades de las personas intervinientes en la actividad de tratamiento afectada por la brecha. El análisis incorpora también una evaluación de los riesgos por la materialización de una posible brecha de seguridad en los datos vinculados al tratamiento.

6.- Entre las medidas reactivas se ha constatado:

- ***(…)***

7.- Entre las medidas preventivas ha quedado constatado:

- ***(…)***

8.- (…).

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad XFERA MÓVILES, S.A.U., es una gran empresa, constituida en el año 2000, con un volumen de negocios de 2.098.178.000 €, en el año 2023.

SEXTO: En fecha 25 de septiembre de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad investigada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD y por la presunta infracción artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

El acuerdo de inicio fue notificado conforme a las normas establecidas en la LPACAP, mediante notificación electrónica, siendo recibido en fecha 27 de septiembre de 2024, como consta en el certificado que obra en el expediente.

SÉPTIMO: Notificado el citado acuerdo de inicio, la entidad investigada presentó escrito de alegaciones en el que, en síntesis, manifestaba que:

PRIMERA. Necesaria suspensión del procedimiento por prejudicialidad penal.
Alega que los hechos objeto de este procedimiento sancionador se encuentran bajo investigación penal, como consecuencia de la denuncia presentada por Xfera ante la Comisaría General de Información de la Policía Nacional, con fecha de 19 de abril de 2023, de la que obra copia en las páginas 245 y siguientes del expediente administrativo.

En concreto, afirma que la investigación ha recaído en el Juzgado de Instrucción n.º 28 de Madrid, y está siendo sustanciada a través de las ***DILIGENCIAS.1, en las que Xfera se ha personado como acusación particular. Acompaña, como Documento n.º 1, copia de la Diligencia de Ordenación por la que se tiene a Xfera por personada en dicho procedimiento. En ella se le informa, además, de que se ha declarado el secreto de las actuaciones, tal y como prevé el artículo 302 de la Ley de Enjuiciamiento Criminal. Sostiene que hasta donde tiene conocimiento, esta declaración ha sido prorrogada en varias ocasiones y se mantiene vigente en la actualidad.

En este caso, considera que nos encontramos ante una situación en la que los mismos hechos están siendo investigados en sede penal, y donde cualquier decisión administrativa prematura podría resultar contradictoria con lo que se resuelva en tal jurisdicción.

Asimismo, destaca que el secreto de sumario declarado en el marco de la investigación penal impide a Xfera acceder a información que podría resultar esencial para la defensa en este procedimiento sancionador. La imposibilidad de acceder a dicha información no solo limita su derecho a la defensa, sino que podría dar lugar a una resolución administrativa basada en hechos que aún no han sido completamente aclarados. Al respecto, el artículo 77.4 de la LPAC establece que los hechos declarados probados en una resolución penal firme vinculan a las administraciones en el marco de los procedimientos sancionadores. Dado que los hechos subyacentes están siendo evaluados en la vía penal, considera que cualquier pronunciamiento administrativo debería suspenderse, a la espera de la pertinente resolución para ofrecer una adecuada seguridad jurídica.

Llegados a este punto, expone que en este procedimiento concurren la triple identidad de sujeto, hecho y fundamento que exige la jurisprudencia para suspender la tramitación de un procedimiento sancionador por prejudicialidad penal:

1. En cuanto a la identidad de sujeto, entiende que es clara, toda vez que Xfera es parte del procedimiento penal, y ha sido considerada como responsable de los hechos en este procedimiento sancionador;

2. En lo tocante a la identidad de hecho, afirma que es indiscutible, pues la investigación en ambos ámbitos se centra en la vulneración de los sistemas de Xfera, que habría dado lugar a la exfiltración de datos de algunos de sus clientes; y

3. Finalmente, considera que concurre igualmente la identidad de fundamento, puesto que en este ámbito se analiza la vulneración del deber de confidencialidad, como infracción principal; y en el otro se investiga un posible delito de revelación de secretos con afectación a datos reservados de carácter personal.

Alega que sujetos, hechos y bienes jurídicos protegidos coinciden en los ámbitos penal y administrativo: no en vano, ambos procedimientos buscan determinar cómo se produjo el ataque informático y si esa vulneración causó algún impacto real a los afectados. Considera que la resolución penal será determinante, por tanto, no solo para atribuir responsabilidades, sino también para evaluar el alcance del daño, lo que condiciona directamente la decisión en este ámbito administrativo y que continuar con el procedimiento sancionador sin esperar el desenlace del proceso penal supondría vulnerar el derecho a la defensa de Xfera, y atentaría contra los principios de seguridad jurídica y de coherencia.

Por consiguiente, considera, que en dicho proceso existe información adicional, no disponible, ni para la AEPD, ni para Xfera cuyo contenido es trascendental para la correcta determinación de los hechos y, en consecuencia, de las responsabilidades que puedan derivarse de los mismos. De esta forma, expone que la continuación del presente procedimiento generaría indefensión a esa parte, en la medida en la que tan sólo dispone de acceso parcial a la documentación e información relativa a supuesto de hecho, con base en el cual se pretende imputarle una infracción de la normativa de protección de datos personales, en gran parte, en base a suposiciones sobre supuestos efectos del incidente de seguridad que, muy probablemente, quedarán esclarecidos en el procedimiento penal, y concretamente, si se produjo, o no, una exfiltración de los datos, más allá de su mera consulta. Así mismo, en particular, considera que esta Agencia dota de relevancia al hecho de la utilización masiva de direcciones IP desde el mismo número como elementos esenciales para la tipificación, calificación y propuesta de sanción como circunstancias agravantes (págs. 37 y 38 del Acuerdo de Inicio), cuyas circunstancias detalladas deben figurar en el expediente del asunto.

Por todo lo expuesto, y en virtud del principio de prejudicialidad penal, solicita que se suspenda el presente procedimiento sancionador hasta que se resuelva el procedimiento penal en curso. Solo entonces afirma que podrá evaluarse correctamente la responsabilidad de Xfera y el impacto real de los hechos investigados sobre los afectados.

SEGUNDA. - SOBRE EL SUPUESTO DE HECHO

Considera que ha de tenerse en cuenta que el sistema VFR estaba dimensionado de tal forma que pudiese escalar de forma automática para poder dar servicio de forma simultánea a un número muy elevado de usuarios, dada cuenta de que en la actualidad la entidad cuenta con un total de más de 1.000 tiendas y era utilizado por más de 11.000 usuarios de diversos servicios de la operadora, que pueden realizar tantas consultas como sean necesarias para atender las peticiones de los clientes;

siendo habitual y recurrente que se produzcan picos de peticiones o las mismas no sean realizadas en horarios de tienda, debido a que Xfera presta servicios de atención al cliente 24 horas al día y que los agentes de tiendas físicas, tratándose de profesionales liberales, con plena autonomía, realizan tareas de gestión en horarios que no son los de tienda, como los que, a juicio de la AEPD y sin aportar evidencia en contra alguna, son situaciones más que habituales en el día a día de Xfera.
Expone que en fecha 29 de marzo de 2023, dentro del proceso de monitorización de Xfera, se detectó un posible comportamiento anómalo de la aplicación Vista4Retail (en adelante, "VFR")1, por lo que, siguiendo los procedimientos internos, se activó un análisis detallado, dando así cumplimiento al procedimiento de gestión de incidentes de seguridad interno, el cual proporciona como Documento n.º 2.

Añade que en fechas anteriores próximas a la incidencia de seguridad que nos ocupa, se realizó un trabajo programado sobre los DNS de la sociedad, que provocó que se habilitase el acceso a VRF por fuera del proxy de autenticación, por lo que quedó expuesto el sistema a su acceso sin el doble factor de autenticación de forma temporal y excepcional.

En línea con lo anterior, pone de relieve que las consultas irregulares provenían de una única cuenta, que se correspondía con un usuario autorizado, debidamente autenticado con credenciales válidas, por lo que afirma que la herramienta gestionó las peticiones de forma ordinaria, sin generar ninguna alerta o detectarse ninguna incidencia de funcionamiento.

Expone que durante una revisión rutinaria efectuada el día 29 de marzo de 2023, se detectó un posible comportamiento anómalo de VFR, lo que provocó que, de forma inmediata, se pusiera en contacto con el titular de dicha cuenta, no reconociendo este ser autor material de las consultas, procediéndose inmediatamente a deshabilitar su cuenta y tratarse el incidente con un potencial ataque contra la seguridad de Xfera.

Así, afirma que la incidencia de seguridad derivó en la realización de consultas a la herramienta VFR de forma irregular, por parte de un usuario legítimo, empleando credenciales válidas, al que el atacante había suplantado la identidad en el sistema.

Informa que el mismo día 29 de marzo de 2023, tras observar que, potencialmente habría tenido lugar un incidente de seguridad, se realizó un análisis de riesgos inicial para los derechos y libertades de los posibles interesados afectados, el cual aporta como Documento n.º 3 y se modificó inmediatamente el procedimiento de identificación/autenticación de los clientes que pudieran referirse a datos potencialmente afectados por el incidente, realizando desde entonces la verificación de la identidad de los clientes por parte de los servicios de atención al cliente y postventa a partir de datos de los que se tenía certeza que no pudiesen estar afectados por las consultas identificadas.

En paralelo, alega que se adoptaron una serie de decisiones destinadas a la contención del ataque y a su posterior resolución. Asimismo, afirma que se implementaron medidas adicionales que ya fueron comunicadas a esta Agencia en la notificación de violación de seguridad de los datos personales y sus posteriores ampliaciones cursadas por Xfera, así como en los requerimientos de información previos al inicio del procedimiento.

Una vez finalizado el análisis completo del incidente, el día 31 de marzo de 2023, expone que se concluyó que, efectivamente, se había producido una violación de seguridad que afectaba a datos personales, e inmediatamente, el mismo día, se procedió a su notificación a la Agencia Española de Protección de Datos a través de la sede del 060 - al no ser posible utilizar el formulario de la Sede electrónica de la Agencia por falta de disponibilidad de este-. Se anexan como prueba de la notificación en plazo de la citada brecha: Documento n.º 4 - 230331 - Justificante notificación brecha y Documento n.º 5 - 230331 - Notificación inicial incidente.

Posteriormente, en cumplimiento del deber de responsabilidad proactiva, afirma que Xfera inició el proceso de comunicación de la violación de seguridad a los interesados, siguiendo las especificaciones para tal comunicación recogidas en el artículo 34 del RGPD al respecto. Para ello informa que se hizo uso prioritariamente de la vía del correo electrónico, y como alternativa, el SMS para aquellos casos en los que el cliente no había aportado un correo electrónico como dato de contacto, o en aquellos casos que no se lograra contactar vía correo electrónico, alcanzándose un total de ***CANTIDAD.3 usuarios efectivamente informados.

Se anexa como Documento n.º 6 - 230331 - Comunicación maquetada el contenido del mensaje enviado a los clientes.

El día 19 de abril de 2023, indica que se procedió a presentar denuncia ante las Fuerzas y Cuerpos de Seguridad los hechos ocurridos y descritos con carácter previo -se adjunta como Documento n.º 7 – denuncia presentada-.

En fecha de 28 de abril de 2023, afirma que se procedió a notificar, dentro del plazo de un mes desde la notificación inicial presentada, notificación de cierre de la violación de seguridad. Se anexa como Documento n.º 8 – 230428 - Justificante comunicación completa, que contiene la citada notificación.

Expone que en la misma se concluye que no constaba, hasta el momento, la filtración de la información comprometida. A fecha actual, informa que no se ha constatado que se haya publicado en abierto ningún dato de los afectados en la Deep Web, ni en Internet, ni se ha publicitado venta de datos obtenidos del incidente sufrido por Xfera. Alega que tampoco se ha detectado ningún tipo de suplantación de identidad, fraude o pérdidas económicas para los clientes afectados frente a Xfera, ni tampoco se ha aportado evidencia alguna por parte de la AEPD, ni de ninguno de los denunciantes en contra.

Afirma que, desde la AEPD, en fecha 12 de mayo de 2023, se remitió el escrito que da cierre a las actuaciones de la División de Innovación Tecnológica en relación con el incidente de seguridad. Se adjunta como Documento n.º 9 - 230512 - Cierre actuaciones división innovación tecnológica, en el que consta que “no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales”

Pese a ello, considera que, concluidas las acciones llevadas a cabo por la División de Innovación Tecnológica de la Agencia sobre el incidente descrito, en las que determinó

que no eran necesarias actuaciones adicionales, la AEPD, apertura expediente e inicia actuaciones de investigación contra Xfera, en relación con la brecha de seguridad.

Se adjunta como Documento n. º10 la información solicitada sobre el incidente.

Expone que, en fecha de 13 de marzo de 2024, se remitió un tercer requerimiento de información, cuya respuesta fue proporcionada por Xfera el día 9 de abril de 2024. Se adjunta dicha comunicación como Documento n.º 11.

Del examen de los hechos relativos al incidente de seguridad arriba relacionados, concluye afirmando que se desprende que la Agencia identifica como constitutivo de infracción, el mero hecho de que se produzca una brecha de seguridad y que se hayan presentado reclamaciones por quienes fueron diligentemente informados de la misma, siendo éste último hecho el único que, en su opinión, hace que la AEPD vuelva a reactivar un procedimiento, respecto al que ella misma había dictado que "*no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales"*, sin que se atienda, ni analice el concreto supuesto de hecho, la ausencia de perjuicio asociado o de publicación en abierto de los datos, las medidas de seguridad implementadas, ni las responsabilidades derivadas.

TERCERA. Vulneración de los principios "non bis in ídem" y de especialidad.

Alega que los hechos que se imputan a Xfera han sido calificados, en el Acuerdo de Inicio, como constitutivos de dos infracciones diferenciadas: por un lado, la vulneración del artículo 5.1.f) del RGPD, tipificada como infracción muy grave, y por otro, el incumplimiento del artículo 32 del RGPD, tipificada como grave.

Considera que el Acuerdo de Inicio explica que la primera sanciona la pérdida de confidencialidad de los datos personales, mientras que la segunda reacciona frente a la insuficiencia de las medidas de seguridad implementadas. Sin embargo, esta calificación resulta, en su opinión, incorrecta, ya que ambas infracciones se aplican sobre una misma conducta y persiguen proteger el mismo bien jurídico, lo que vulnera los dos principios expuestos.

3.1. Vulneración del principio non bis in ídem

Afirma que en el caso que nos ocupa, las dos infracciones propuestas por la Agencia buscan sancionar la misma conducta: la supuesta falta de adopción de medidas técnicas y organizativas suficientes para garantizar la seguridad de los datos personales. No existe, por tanto, en su opinión, una pluralidad de conductas que pueda justificar la doble sanción.

Expone que en el caso de Xfera, la conducta sancionada, que es la falta de adopción de medidas de seguridad adecuadas, ha provocado la pérdida de confidencialidad: sin una, no se habría producido la otra. Considera que ambas infracciones, por tanto, derivan de la misma conducta y se relacionan con el mismo bien jurídico, lo que refuerza la idea de que la doble sanción vulnera el principio non bis in ídem.

Indica que es claro que, ambas infracciones sancionan el mismo hecho: la supuesta insuficiencia de las medidas de seguridad adoptadas para evitar el acceso no autorizado a los datos personales. Esta falta de diferenciación entre los hechos sancionados en cada infracción es precisamente lo que le lleva a concluir que se ha vulnerado el principio non bis in ídem.

Dicho lo anterior, también tiene conocimiento de que la AEPD sí ha aplicado este principio en procedimientos como el PS/00027/2021 o el PS/00021/2021. En tales casos, aun existiendo una brecha de confidencialidad derivada de la implementación de insuficientes medidas de seguridad, considera que la AEPD decidió sancionar únicamente por infracción del artículo 5.1.f) del RGPD.

3.2. Vulneración del principio de especialidad

Alega que el artículo 32 es la norma que se ajusta con mayor precisión a los hechos objeto de este procedimiento, ya que regula de forma detallada las medidas técnicas y organizativas que deben implementarse para garantizar un nivel de seguridad adecuado al riesgo. Y que, por el contrario, el artículo 5.1.f), al ser una disposición más general, debe ceder ante la aplicación de la norma especial, que contempla de manera más específica el comportamiento ilícito.

En el presente caso, considera que el artículo 32 del RGPD regula de manera más precisa las obligaciones de seguridad cuya vulneración se atribuye a Xfera, mientras que el artículo 5.1.f) se limita a enunciar un principio general. Por tanto, afirma que la correcta aplicación del principio de especialidad exige que la conducta de Xfera sea sancionada únicamente bajo el artículo 32, y que se excluya la aplicación del artículo 5.1.f).

En definitiva, entiende que la doble calificación realizada en el Acuerdo de Inicio no se ajusta a derecho, ya que vulnera tanto el principio non bis in ídem como el principio de especialidad. Expone que la conducta antijurídica sancionada es única, y debe ser subsumida en el artículo 32 del RGPD, que es la norma que más exactamente se ajusta a los hechos y que aplicar tanto el artículo 5.1.f) como el artículo 32, no solo es contrario a la doctrina del TJUE y del Tribunal Supremo, sino que también resulta desproporcionado, tal y como ha subrayado el Comité Europeo de Protección de Datos en sus Directrices sobre el cálculo de sanciones.

Por todo lo expuesto, solicita que, en la resolución definitiva, se desestime la aplicación del artículo 5.1.f) del RGPD al procedimiento que nos ocupa, y que los hechos se califiquen exclusivamente como una infracción del artículo 32 del mismo Reglamento, de acuerdo con los principios antes expuestos.

CUARTA. La actuación de Xfera fue diligente; adecuación y correcta implementación de las medidas de seguridad.

Entrando en el fondo del asunto, alega que el presente expediente trae causa de un incidente de seguridad que fue identificado por los procesos internos de monitorización de la empresa, que detectaron un comportamiento anómalo a través de una aplicación utilizada en sus servicios de interacción con clientes (puntos de venta, call centers, atención al cliente, etc.). Estas consultas, afirma, que fueron realizadas con

credenciales válidas de un usuario autorizado, quien manifestó no haber realizado dicha actividad. Manifiesta que, de manera inmediata, Xfera desactivó la cuenta y trató el incidente como un posible ataque de exfiltración de datos.

Expone que Xfera respondió con celeridad al detectar la brecha, activando las medidas necesarias para restaurar la seguridad del sistema y notificando tanto a la AEPD como a los clientes afectados y complementando esta información con posterioridad. Alega que, durante todo el proceso, la empresa siguió los protocolos establecidos a tal efecto, implementando mejoras significativas en sus políticas de seguridad para evitar que incidentes similares se repitan en el futuro. Le sorprende que esta autoridad considere las medidas reactivas adoptadas tras la brecha como una prueba de insuficiencia preventiva: todo lo contrario, en su opinión son una muestra del compromiso de Xfera con la protección de los datos personales y la mejora continua de sus sistemas.

4.1. Las medidas implementadas por Xfera eran adecuadas.

Expone que, para llevar a cabo dicha actividad de tratamiento, se efectuó, en su momento, el correspondiente análisis de riesgos, que aporta dentro del Informe detalle tratamiento Enrollment como Documento n.º 12.

Como acreditación de la instauración de las medidas de seguridad citadas, más concretamente la del Doble factor de autenticación, aporta de nuevo como Documento n.º 13 - Implementación IAP Google + 2FA VFR distribuidor.

(…)

Reitera que la herramienta afectada por el incidente de seguridad habilita la operativa principal de los agentes que atienden a los clientes, teniendo una función de “directorio” o “buscador”. A través de esta, se les permite efectuar consultas sobre los clientes, es decir, se trata de un buscador que gestiona las funciones diarias llevada a cabo por los agentes de esta operadora en diversos canales, que constituyen la base de su actividad de negocio y comercial.

Lo anterior desea que sea puesto en contexto por esta Agencia; especialmente a la hora de identificar posibles medidas que resulten aplicables toda vez que no cabe que la misma estuviera sometida a un cifrado o a ciertas medidas excesivamente restrictivas ya que, se estaría interrumpiendo drásticamente – por no decir impidiendo- la dinámica de atención a los clientes y potenciales clientes, que verían imposibilitadas sus labores. En definitiva, alega que no es viable operativamente, para ninguna entidad, bloquear la herramienta de iteración básica del dealer o agente en su operativa ordinaria.

Concluye afirmando que se trata de una herramienta concebida para permitir realizar consultas de forma masiva y de forma escalable y, siendo esta la principal virtud y finalidad para la que fue diseñado, contraprogramar esta funcionalidad implicaría un altísimo conste económico, técnico y de tiempo.

4.2. No es razonable interpretar las medidas reactivas como insuficiencia preventiva.

Manifiesta que al tratarse de un ataque que utilizaba credenciales legítimas sobre un sistema con alta carga de consultas legítimas, la detección era más difícil. A pesar de ello, una vez identificado el problema, expone que Xfera adoptó medidas reactivas no solo para contener el daño, sino para reforzar la seguridad del sistema, práctica habitual en ciberseguridad, ya que la mejora continua forma parte de todos los estándares de seguridad conocidos.

Considera evidente que el hecho de que Xfera haya implementado medidas adicionales, como la mejora de los sistemas de monitorización y la revisión de las políticas de autenticación, no debe considerarse como una admisión de que las medidas preventivas originales fueran insuficientes. Afirma que estas acciones responden al deber de diligencia que impone el RGPD, que obliga a los responsables del tratamiento a revisar y mejorar sus políticas de seguridad en función de las amenazas detectadas. Expone que la capacidad de una empresa para aprender de un incidente y ajustar sus mecanismos de protección es precisamente lo que garantiza una mayor seguridad para los datos de los clientes en el futuro. Penalizarla por ello se le antoja, cuanto menos, contraproducente, y contrario a las Directrices 04/2022 del CEPD, según las cuales la cooperación de la empresa, su capacidad para rectificar y mejorar tras un incidente, y su cumplimiento con el principio de responsabilidad proactiva deben influir positivamente en la cuantificación de la sanción final.

4.3. La retirada del IBAN de la aplicación VFR se realizó para evitar futuros fraudes.

Alega que la rápida implementación de una medida que reforzó la autenticación tras la brecha demuestra un claro compromiso con la protección de los derechos de los interesados, lo que no solo redujo el riesgo de suplantación de identidad, sino que también evitó que uno de los datos comprometidos (el IBAN) pudiera ser utilizado de forma fraudulenta en el futuro.

Considera que este enfoque, consistente en sustituir un dato vulnerado por otro no vulnerado, tras identificar un riesgo concreto, entra dentro de las acciones que el CEPD valora para mitigar los daños y perjuicios sufridos por los interesados. Por tanto, afirma que la retirada del IBAN como dato de autenticación no debe verse como una admisión de que su uso inicial era inadecuado, sino como una respuesta responsable que contribuye a paliar los posibles daños, lo que debe actuar como factor atenuante al evaluar la gravedad de la infracción.

4.4. Del cierre de actuaciones por la División de Innovación Tecnológica de la AEPD.

Expone que, en fecha de 12 de mayo de 2023, se recibe un escrito de la Agencia, por el cual se concluyen las actuaciones relacionadas con la brecha de seguridad que nos ocupa por la División de Innovación Tecnológica.

Afirma que la División de Innovación Tecnológica de la Agencia es la sección técnica que examina el cumplimiento y la gestión de las brechas de seguridad, conforme a la normativa de protección de datos de carácter personal. Alega que de su propio análisis se concluye que no es necesaria la realización de actuaciones adicionales, en la medida en la que Xfera ha actuado conforme a sus obligaciones, notificando a la autoridad y a los interesados, brindando a éstos la información pertinente y el soporte que pudiesen precisar.

4.5. Xfera como víctima de una actuación criminal respecto a la que se ha decretado secreto de sumario.

Reiterar la importancia de situar correctamente a Xfera en su posición de víctima de un ataque criminal instrumentado a través de un altamente complejo, interviniendo finalmente, como ya ha sido puesto de manifiesto, las Fuerzas y Cuerpos de Seguridad.

Considera que este enfoque no debe ser obviado, en la medida en la que, la Agencia debe contemplar que, pese a un despliegue de medidas adecuado y diligente, cabe la posibilidad de que, pese a ello, el Responsable del Tratamiento sea víctima de una brecha de seguridad, la cual, debe ser gestionada de forma correcta, como prevé la propia normativa de protección de datos, pero en su opinión no puede considerarse, de forma automática, que el propio acontecimiento de la brecha, de forma autónoma, determine una falta de negligencia de la entidad afectada, en la medida en la que ésta viene provocada por la actuación criminal de un tercero, que ya está siendo investigada, consiguientemente, en la vía penal.

4.6. Conclusión: vulneración del principio de culpabilidad.

Concluye que al no haberse acreditado la concurrencia de una actuación culpable, intencionada o negligente por parte de Xfera no procede la identificación en la conducta de esa parte de una infracción de la normativa de protección de datos personales por el mero hecho de haber sido víctima de un acto delictivo y, consecuentemente, considera que no procede la imposición de ningún tipo de sanción.

Afirma que sólo es posible sancionar administrativamente con base en el RGPD cuando haya quedado debidamente acreditada por parte de la autoridad administrativa competente la concurrencia de una actuación culpable, intencionada (dolosa) o negligente por parte de responsable de tratamiento, algo que en su opinión no ha sucedido en el presente procedimiento.

Es por ello por lo que considera que el presente Acuerdo de Inicio no es ajustado a derecho, pues impone a XFERA una obligación de resultado, consistente en el establecimiento de medidas infalibles, al imputar una infracción del artículo 5.1 apartado f) y del artículo 32 del RGPD, basándose únicamente en el resultado que se produce por la actuación criminal de un tercero, sin atender a la diligencia utilizada y sin considerar el despliegue de medidas técnicamente adecuadas e implantadas.

En este sentido, resalta que la implementación de medidas inquebrantables, ni es viable, puesto que toda medida por muy segura que sea, y cuente con las garantías e incluso certificaciones de seguridad oportunas, tiene vulnerabilidades; ni es exigible por la normativa que resulta de aplicación.

En el caso que nos ocupa, alega que no hay indicios de que la empresa actuara de forma negligente. De hecho, afirma que la información obrante en el expediente muestra lo contrario: Xfera implementó medidas preventivas razonables, como el uso del doble factor de autenticación (2FA) y la monitorización de sus sistemas. Expone que el incidente de seguridad se produjo debido a una operación técnica sobre la

configuración del DNS, que permitía el acceso evitando el proxy de autenticación de VFR. Indica que este fallo técnico no puede considerarse negligente, ya que se trató de un incidente aislado y no de una falta sistemática de seguridad. Además, tras la detección de la brecha, manifiesta que Xfera actuó con celeridad para mitigar los daños, notificando a la AEPD y a los afectados dentro de los plazos establecidos y adoptando medidas adicionales para reforzar su sistema de seguridad.

En definitiva, considera vulnerado el principio de culpabilidad, al imputar a Xfera una infracción basada exclusivamente en el resultado del ataque, sin demostrar la existencia de negligencia o dolo en su actuación y que las medidas adoptadas por Xfera antes y después del incidente demuestran que la empresa cumplió con su obligación de medios, y no se puede exigir una seguridad infalible. En este sentido, solicita que se tenga en cuenta el principio de culpabilidad y que, en caso de que se aprecie algún grado de responsabilidad, se valore la imposición de una sanción menos gravosa, como el apercibimiento, de acuerdo con el artículo 58.2.b) del RGPD y el artículo 76.3 de la LOPDGDD.

QUINTA. Falta de proporcionalidad de la sanción.

Alega que, en el presente caso, la AEPD ha propuesto una sanción de 4.000.000 euros, una cuantía claramente desproporcionada teniendo en cuenta las circunstancias del caso y las medidas adoptadas por Xfera tanto antes como después de la ocurrencia del incidente. Considera que esta cifra no refleja una evaluación adecuada del impacto real del incidente ni de las acciones correctivas adoptadas por la empresa, que ha demostrado su compromiso con la mejora continua de sus sistemas de seguridad.

De entrada, entiende oportuno insistir en que sancionar tanto por el artículo 5.1.f) como por el 32 genera una carga punitiva desproporcionada, pues la pérdida de confidencialidad derivada de una brecha de seguridad ya está contenida en la infracción relacionada con las medidas de seguridad. Afirma que la AEPD justifica la sanción separada sobre la base de la gravedad de la pérdida de confidencialidad, pero al sancionar la causa y el efecto de la misma infracción, se está duplicando injustificadamente la penalización, lo que, en su opinión, vulnera el principio de proporcionalidad.

Entiende que, en este caso, una sanción de 4.000.000 euros no solo resulta desproporcionada en relación con los hechos, sino que tampoco se ha acreditado que sea necesaria para lograr los fines disuasorios.

Por tanto, solicita que, a la luz del principio de proporcionalidad, se reduzca la sanción impuesta a Xfera. Argumenta que la empresa ha demostrado una voluntad proactiva para corregir la situación, implementando mejoras significativas en sus sistemas de seguridad, lo que debería ser tenido en cuenta a la hora de graduar la sanción. Considera que la imposición de una sanción más moderada no solo sería adecuada, sino que también respetaría los principios de necesidad e idoneidad consagrados en la Ley 40/2015.

SEXTA. Circunstancias aplicables al caso individual, conforme al art. 83.2 RGPD.

6.1. Naturaleza, gravedad y duración de la infracción.

Afirma que, en este caso, no se ha acreditado que ninguno de los afectados haya sufrido daño alguno a consecuencia de la exfiltración de los datos.

Manifiesta que Xfera ha reforzado sus servicios de vigilancia digital, que monitorizan de forma continua la Deep web y varios foros frecuentados por delincuentes digitales, en busca de cualquier dato que pudiera estar relacionado con la exfiltración. Informa que, hasta la fecha, no se ha detectado ningún indicio de intentos de vender o utilizar los datos para fines ilícitos.

Lo anterior desea poner en relación con el hecho de que el incidente fue detectado a través de las propias medidas de seguridad implementadas por Xfera, lo que permitió reaccionar de forma efectiva para limitar su duración.

Considera que esta detección fue clave para que se pudiera intervenir con prontitud, conteniendo el impacto de la brecha y minimizando el tiempo en que los datos estuvieron expuestos, lo que entiende que debería ser tenido en cuenta igualmente por esta Agencia, a los efectos de moderar la sanción propuesta.

6.2. De la ausencia de perjuicio para los interesados afectados por la brecha.

Expone que la Agencia realiza una manifestación genérica sobre posibles efectos de la brecha que no responden a la realidad de los hechos probados, sin concretar en modo alguno qué reclamaciones o interesados considera víctimas de phishing. Indica que, en concreto, se han interpuesto 8 reclamaciones contra XFERA, de entre los ***CANTIDAD.3 interesados a los que se notificó (lo que supone el 0,00049984 del total de notificados).
Se aporta como Documento n.º 14, siquiera resumidamente, la realidad de lo que consta en el expediente en relación con las reclamaciones presentadas.

Afirma que ningún reclamante relata ni señala (ni, en ningún caso consta acreditada) la existencia perjuicio alguno relacionado con la brecha, ni económico ni material y que no consta la existencia de perjuicio material o económico como resultado de la brecha de seguridad de XFERA.

6.3. Intencionalidad o negligencia en la sanción.

No niega que el incidente estuvo relacionado con un problema con la configuración del DNS, pero desea señalar que se trató de una cuestión puntual, y no del resultado de una negligencia grave o de una omisión sistemática en las medidas de seguridad. Afirma que la causa fue una actuación sobre la infraestructura de DNS, y no la falta de previsión o a la inexistencia de medidas de seguridad adecuadas que se le atribuye. Añade que, de hecho, antes del incidente, Xfera había implementado medidas avanzadas de seguridad, como el doble factor de autenticación (2FA), que no hacen sino acreditar su esfuerzo por dotarse de unas medidas de seguridad sólidas.

Considera que las medidas de seguridad implementadas antes del incidente, junto con la rápida respuesta tras su detección, demuestran que Xfera actuó con la diligencia necesaria y en cumplimiento de sus obligaciones.

6.4. Medidas adoptadas para paliar los daños y perjuicios sufridos por los interesados.
Entiende oportuno destacar, igualmente, que en cuanto tuvo conocimiento de la existencia del ataque, Xfera adoptó medidas efectivas para mitigar los daños causados por la brecha de seguridad. Manifiesta que esta reacción rápida y espontánea, tal como señalan las Directrices 04/2022 del CEPD, es un factor que debe considerarse atenuante, dado que demuestra, en su opinión, que Xfera actuó de forma proactiva antes de cualquier acción por parte de la autoridad de control.

Finalmente, concluye afirmando que Xfera no se limitó a paliar los daños inmediatos, sino que también implementó mejoras en sus sistemas de seguridad para prevenir futuros incidentes. Considera que estas acciones correctivas, como el refuerzo de las reglas de monitorización y la adopción de nuevas medidas de control, demuestran la diligencia de Xfera y su compromiso con la mejora continua y que, en conjunto, estas medidas demuestran que Xfera hizo todo lo posible para limitar las repercusiones del incidente y proteger a los afectados, lo que, según las Directrices del CEPD, debería ser considerado, en su opinión, un factor atenuante en la evaluación de la sanción.

6.5. Infracciones anteriores cometidas por Xfera.

Destaca que en relación con la posible consideración de las resoluciones PS-00448-2020, PS-00237-2019, y PS-00104-2020 como precedentes en este procedimiento, dichas infracciones estarían prescritas, por lo que no deberían ser tenidas en cuenta.

Entiende que las diferencias en el alcance y la naturaleza de los expedientes mencionados por la Agencia limitan su aplicabilidad como precedentes al caso que nos ocupa. Todo ello, de acuerdo con el párrafo 88 de las Directrices 04/2022 del CEPD, según el cual las infracciones anteriores relacionadas con un mismo objeto pueden considerarse más pertinentes que las que abordan cuestiones distintas, como son las tres indicadas por la Agencia. De ahí que considere que no es razonable utilizar estos precedentes como agravantes, a efectos del cálculo de la sanción.

6.6. Adhesión a códigos de conducta o a mecanismos de certificación aprobados.

Alega que Xfera cuenta con las certificaciones ISO 27001 de Seguridad de la Información y 27701 de Gestión de la Privacidad de la Información, así como Esquema Nacional de Seguridad nivel Alto, lo que, en su opinión, acreditaría el cumplimiento por parte de la empresa de los más altos estándares de seguridad de la información, circunstancia que es auditada periódicamente.

Se aportan como Documento n.º 15 y Documento n.º 16 las certificaciones referidas a Xfera móviles S.A.U. en cuanto a la ISO 27001 y a la ISO 27701. Así mismo se aporta el certificado, como Documento n.º 17, correspondiente a la certificación ENS nivel Alto de Xfera.

Adicionalmente, informa que Xfera se encuentra adherida al Código de Conducta de Tratamiento de Datos en la Actividad Publicitaria, siendo esto reflejo de su compromiso con el cumplimiento de los más altos estándares en materia de protección de datos.

SÉPTIMA. Proposición de prueba.

En orden a la acreditación de los hechos, solicita la apertura del periodo probatorio en el que sean admitidos y practicados los siguientes medios de prueba:

1. Documental, consistente en la unión al procedimiento de los documentos aportados;

2. Pericial, a realizar por ***J.J.J.*** y ***L.L.L.***, ambos Profesores titulares de la Universidad de ******LOCALIDAD.1***, y cuyo ámbito, detallado en la carta de aceptación de encargo que se anexa como Documento n.º 18, se referirá al análisis de las medidas de seguridad de Xfera que pudiesen ser de interés en relación con este procedimiento. Informa que este informe está siendo redactado en la actualidad, y será aportado a esta Agencia a la mayor brevedad, al amparo de lo previsto en el artículo 76.1 de la LPAC.

Por todo lo expuesto, solicita que se proponga el archivo de las actuaciones en la propuesta de resolución que se redacte, debido a la ausencia de culpabilidad y a la no vulneración del principio de exactitud. Subsidiariamente, en atención a la cualificada disminución de la culpabilidad concurrente en Xfera, se imponga únicamente una sanción de apercibimiento y subsidiariamente, se proponga unas sanciones más leves que las incluidas en el Acuerdo de inicio de procedimiento sancionador.

OCTAVO: En fecha 4 de marzo de 2025 y con número de registro de entrada REGAGE25e00014827098Se, se ha recibido en esta Agencia, la reclamación formulada por ***M.M.M.***, referida a XFERA MÓVILES, S.A.U. en la que afirma que, siendo cliente de la operadora de telefonía reclamada, el 2 de abril de 2023, recibió una comunicación de esta en la que le informaban que habían experimentado un incidente por el cual, terceras personas ajenas a la organización podrían haber accedido a algunos de los datos que tratan de él como cliente. Refiere que desde ese momento no para de recibir comunicaciones de spam con multitud de enlaces maliciosos o fraudulentos.

En fecha 11 de abril de 2025, se admitió a trámite la reclamación formulada.

NOVENO: En fecha 24 de junio de 2025, se formuló propuesta de resolución, proponiendo:

<<Que por la Presidencia de la Agencia Española de Protección de Datos se sancione a XFERA MÓVILES, S.A.U., con NIF A82528548,

- por la infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción, en el artículo 72.1 a) de la LOPDGDD, con una multa de 2.500.000 euros.

- por la infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción, en el artículo 73 f) de la LOPDGDD, con una multa de 1.500.000 euros. >>

La citada propuesta de resolución fue enviada, conforme a las normas establecidas en la LPACAP, mediante notificación electrónica, siendo recibida en fecha 25 de junio de 2025, como consta en el certificado que obra en el expediente.

DÉCIMO: En fecha 26 de junio de 2025, XFERA MÓVILES presentó un escrito a través del cual solicitaba la ampliación del plazo conferido para presentar alegaciones. En fecha 30 de junio de 2025, el órgano instructor del procedimiento acordó la ampliación de plazo hasta un máximo de cinco días, que debían computarse a partir del día siguiente a aquel en el que finalizara el primer plazo de alegaciones El citado acuerdo fue notificado en fecha 1 de julio de 2025, como consta en el acuse de recibo que obra en el expediente.

UNDÉCIMO: En fecha 16 de julio de 2025, XFERA MÓVILES presentó escrito de alegaciones a la Propuesta de Resolución, reiterando básicamente las alegaciones ya presentadas ante el Acuerdo de Inicio y en el que, en síntesis, manifiesta que:

PRIMERA. - DE LA NECESARIA SUSPENSIÓN DEL PROCEDIMIENTO POR PREJUDICIALIDAD PENAL.

Considera jurídicamente improcedente (y potencialmente lesivo para el derecho de defensa de XFERA) continuar con la tramitación y resolución del procedimiento sancionador mientras permanezca abierta y no resuelta la causa penal 1471/2023, actualmente en instrucción en el Juzgado de Instrucción n.º 28 de Madrid.

Por ello, en aplicación de los artículos 22.1.g) y 77.4 de la LPACAP, solicita a la Agencia Española de Protección de Datos que suspenda el presente procedimiento sancionador hasta que se dicte resolución firme en el procedimiento penal actualmente en curso.

Aporta de nuevo Documento n.º 1, Diligencia de Ordenación del Juzgado y Documento n.º 2 – Denuncia policial presentada por XFERA.

SEGUNDA. - DE LA INSTRUCCIÓN DEL EXPEDIENTE ADMINISTRATIVO POR LA AGENCIA.

Manifiesta que el incidente fue notificado por XFERA el 31 de marzo (Documento n.º 3 – Justificante notificación brecha (31.03.2023)) tanto a la AEPD como a los interesados (Documento n.º 4 – Comunicación maquetada (31.03.2023).

Reitera que la actuación de XFERA fue valorada por la propia División de Innovación Tecnológica de la AEPD, que el 12 de mayo de 2023 acordó el cierre de actuaciones (el cual se proporciona como Documento n.º 5 – Cierre actuaciones DIT (12.05.2023)), al considerar que no procedía adoptar medidas adicionales tras la notificación y que la entidad había actuado conforme a sus obligaciones legales y concretamente con lo dispuesto en los artículos 33 y 34 del RGPD (véase el Documento n.º 6 – Respuesta noviembre 2023).

Del examen de los hechos relativos al incidente de seguridad, incide en que la Agencia identifica como constitutivo de infracción el mero hecho de que se produzca una brecha de seguridad y que se hayan presentado reclamaciones por quienes fueron diligentemente informados de la misma.

Considera que la tramitación del presente expediente comporta una serie de irregularidades que le generan indefensión:

- Al considerar como probados hechos sobre los que no consta acreditación, como es la supuesta filtración de la información afectada por la brecha.
- Al no haber admitido a trámite las reclamaciones que constan en el expediente, negando a esta parte la posibilidad de oponerse a ello.
- Negando la relevancia y valoración realizada por la DIT con relación a la incidencia acaecida, en contra de las funciones que ésta tiene atribuidas por el propio Estatuto de la Agencia, y que aplica de forma habitual, tal y como consta recogido en la Memoria de la Agencia.

Por ello, considera que la Propuesta de Resolución no resulta ajustada a derecho, procediendo el archivo de las presentes actuaciones.

TERCERA. - SOBRE LA SUPUESTA INFRACCIÓN DEL ARTÍCULO 5.1. F) DEL RGPD.

Indica que la Agencia debe sancionar de conformidad con los principios de la potestad sancionadora de la Administración Pública, que no deben confundirse con la facultad de actuar de forma arbitraria. Así, se requiere que, en aras de lograr la seguridad jurídica del administrado, la actuación sancionadora de la Administración mantenga criterios de coherencia, intentando no contradecirse o aplicar criterios o baremos distintos en cada resolución.

En su opinión manifiesta que queda sobradamente acreditado que XFERA contaba con medidas adecuadas, pertinentes y proporcionadas, -que se detallan de nuevo en la siguiente alegación- y que la brecha de seguridad acaecida no hubiera podido evitarse dada su naturaleza. Esto pone de manifiesto que, en su opinión, aunque se produjo una brecha de confidencialidad, la compañía actuó de manera diligente, adoptando medidas de seguridad adecuadas antes y después de la misma, por lo que no se produjo un incumplimiento del principio de integridad y confidencialidad (art. 5.1.f RGPD).

3.1 XFERA como víctima de una actuación criminal.

Reitera ante esta Agencia que, la brecha que nos ocupa fue acometida por delincuentes, quienes, infringiendo lo dispuesto en los artículos 264 y 264 bis de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, decidieron llevar a cabo tal intromisión, aun a sabiendas de la pena de prisión que conlleva tal conducta, la cual podría ascender a de dos a cinco años, así como una multa del tanto al décuplo del perjuicio ocasionado. En este sentido, informa que la misma fue presuntamente perpetrada por una persona que ha sido detenida como consecuencia de sus actos y que está actualmente en proceso de ser juzgada para responder de sus responsabilidades penales.

De este modo, expone que, pese al establecimiento de diversas medidas de seguridad, por muy alta que sea la inversión y medios dedicados por las empresas para prevenir los ciberataques, en absoluto es posible detectar y precaver en su

totalidad las nuevas oleadas de ataques, que cada vez son más continuas, complejas e imprevisibles.

Por todo lo anterior, reitera la importancia de situar correctamente a XFERA en su posición de víctima de un ataque criminal instrumentado a través de un altamente complejo, interviniendo finalmente, como ya ha sido puesto de manifiesto, las Fuerzas y Cuerpos de Seguridad.

De ahí que llegue a la conclusión de que, al no haberse acreditado la concurrencia de una actuación culpable, intencionada o negligente por parte de XFERA, no proceda en su opinión la identificación en la conducta de esa parte de una infracción de la normativa de protección de datos personales por el mero hecho de haber sido víctima de un ciberataque, y, consecuentemente, no proceda la imposición de ningún tipo de sanción, todo ello teniendo en consideración la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) relativas a los asuntos C-683/21 (Nacionalinis visuomenės sveikatos centras) y C-807/21 (Deutsche Wohnen) publicada el día 5 de diciembre de 2023 ya que, en caso contrario, entiende que se estaría aplicando la responsabilidad objetiva.

En definitiva, considera vulnerado el principio de culpabilidad y responsabilidad objetiva, al imputar a XFERA una infracción basada exclusivamente en el resultado del ataque, sin demostrar la existencia de negligencia o dolo en su actuación. Considera que las medidas adoptadas por XFERA antes y después del incidente demuestran que la empresa cumplió con su obligación de medios, y no se puede exigir una seguridad infalible.

CUARTA. - SOBRE EL SUPUESTO INCUMPLIMIENTO DE LO DISPUESTO EN EL ARTÍCULO 32 DEL RGPD.

Considera necesario reiterar que el incidente de seguridad fue identificado por los procesos internos de monitorización de XFERA, tras detectar un comportamiento anómalo a través de una aplicación utilizada en sus servicios de interacción con clientes.

4.1. De la adecuación de las medidas implementadas por XFERA.

Tal y como expuso en las medidas de seguridad ya facilitadas a esta Agencia, alega que el código OTP o las medidas de doble factor de autenticación no son exigibles de forma general para una validación de la autenticación de los usuarios en entidades del sector de las Telecomunicaciones.

En el supuesto que nos ocupa, indica que XFERA no sólo detecta de forma proactiva el acceso, sino que lo hace de forma temprana. Considera que este hecho debe ser puesto en contexto por la AEPD, ya que, la detección de una brecha de estas características en el término de días resulta extremadamente inusual, dada la elevada complejidad de la misma, siendo sólo posible con una proactividad y medios como los aplicados por parte de XFERA en cumplimiento del principio de responsabilidad proactiva y diligencia debida. Manifiesta que lo anterior debe ser tenido en cuenta como un resultado de la adecuación de las medidas de seguridad implantadas por XFERA, las cuales, se enumeran de nuevo.

Aporta análisis de riesgos, dentro del Informe detalle tratamiento Enrollment como Documento n.º 7.

En este sentido, considera que a pesar de que la AEPD hace alusión de forma reiterada a lo largo de la Resolución al número de IPs desde las que el atacante realiza su conexión, este hecho no es especialmente relevante desde el punto de vista de la seguridad.

En concreto, explica que las comunicaciones entre la base de datos central del aplicativo VFR y las tiendas está protegida mediante el protocolo HTTPS (Hypertext Transfer Protocol Secure), que significa "Protocolo de Transferencia de Hipertexto Seguro" que cifra la información que se transmite, lo que implicaría que, en caso de ser interceptada por un usuario no autorizado, no tendría posibilidad de acceder al contenido de la misma.

Adicionalmente, expone que la base de datos central que alojaba los datos que VFR ponía a disposición de sus usuarios autenticados estaba también debidamente cifrada.

Por lo tanto, afirma que sí se aplicaban medidas de cifrado a los datos personales para evitar su acceso por parte de usuarios no autorizados. Ocurre que, en este caso, el usuario estaba haciendo uso del aplicativo con unas credenciales válidas, por lo que tenía acceso a la información.

En resumen, considera que las supuestas soluciones que plantea la AEPD, más allá de su idoneidad teórica, no son realistas desde un punto de vista técnico u operativo, teniendo además en cuenta la excepcionalidad del tipo de ataque sufrido, que no cuenta con precedentes conocidos en cuanto a su forma de ejecución y complejidad.

Como se indicaba, manifiesta que la causa de la brecha no puede atribuirse a una deficiencia en las medidas preventivas en sí mismas, sino a una operación técnica aislada, puntual y única que tuvo lugar el 21 de febrero de 2023. Durante ese día, un empleado de XFERA aplicó una configuración desactualizada del sistema DNS, lo que provocó que temporalmente no fuese obligado acceder a VRF a través del proxy de autenticación que gestionaba el doble factor de autenticación. Esta circunstancia permitió que, durante el período entre el 21 de febrero y el 29 de marzo de 2023, fuesen posibles las consultas a los datos únicamente con usuario y contraseña, sin requerir el segundo factor de autenticación.

No obstante, subraya que este hecho no implica una falta estructural de medidas de seguridad, sino que con independencia de que esta medida se hubiera inhabilitado se mantenían otras que, conforme a los riesgos identificados, debieran ser suficientes para la adecuada protección de los datos personales.

Expone que la brecha no deviene de la falta del doble factor de identificación, sino de la obtención por el atacante, de una forma que no se ha podido determinar, de las credenciales de un usuario legítimo. En este sentido, no se está en posición de afirmar, tampoco por la AEPD, que si el doble factor hubiese estado vigente se habría abortado la posibilidad del ataque, ya que dicha medida no es infalible y podría haber estado igualmente comprometida.

Por todo ello, considera que lo que debe valorarse no es la existencia o no de una medida concreta, sino la adecuación de las medidas conforme a las amenazas identificadas y su nivel de riesgo.

En este sentido, indica que la AEPD no ha tenido en consideración en su Resolución la jurisprudencia del Tribunal Supremo aportada en el entorno de las alegaciones al acuerdo de inicio del presente procedimiento sancionador y reiterada en este escrito. En concreto, la sentencia 543/2022 de 15 de febrero de 2022, la cual es clara al afirmar que la adopción de medidas de seguridad en el tratamiento de datos personales no puede considerarse una obligación de resultado, sino una obligación de medios.

Incide en que la eventualidad que provocó este caso fue causada por la aplicación de un archivo desactualizado de configuración, que restauró una versión anterior del DNS, desactivando el proxy de autenticación. Este tipo de incidentes, aunque indeseables, son difícilmente evitables en cualquier proceso tecnológico complejo, y no reflejan una negligencia en las medidas preventivas adoptadas por la empresa.

Por último, reitera que en el supuesto analizado no consta acreditado que se haya producido una exfiltración de los datos. Aunque hay sospechas de ello, conforme a la información facilitada por la Policía tras la denuncia, este extremo no ha sido confirmado. Por lo que entiende que la AEPD, no puede apoyarse en un hecho no probado para tratar de agravar los hechos acaecidos, ni mucho menos la sanción a imponer.

Considera que sí existía una correcta identificación, análisis y valoración del riesgo, ya que la herramienta VRF, así como sus aplicativos complementarios, contaban con todas las medidas oportunas para mitigar los riesgos asociados al tratamiento, debidamente identificados, dando cumplimiento asimismo a lo dispuesto en el artículo 32 del RGPD. Así pues, entiende que, porque el 2FA se encontrara deshabilitado, no puede colegirse una sanción por incumplimiento del artículo 32 del RGPD toda vez que es una medida adicional, no aplicable conforme al análisis de riesgos realizado y que, ni mucho menos, resulta legalmente exigible a las actividades desarrolladas por las operadoras de telecomunicaciones.

Pero, aunque se admitiese que el doble factor fuera necesario, afirma que su desactivación no respondió a un acto intencionado, sino que deriva de una actuación incorrecta de un usuario cualificado, el programador encargado de una actualización, cuya probabilidad de producirse es ínfima. Este desafortunado incidente se ve acompañado de una pérdida de la confidencialidad de las credenciales de un usuario legítimo. En su opinión, la probabilidad de que ambas situaciones se diesen de forma combinada en el tiempo era prácticamente nula, por lo que no puede inferirse de esta circunstancia, tan absolutamente impredecible e improbable, una falta de diligencia por parte de XFERA.

En definitiva, manifiesta que XFERA ha demostrado su compromiso con la seguridad de los datos y con la mejora continua de sus sistemas de protección, en línea con el principio de responsabilidad proactiva establecido en el RGPD. Considera que la rápida respuesta de la empresa, junto con las mejoras implementadas, refuerzan la idea de que, incluso en un entorno de alta actividad como el de la aplicación VFR,

XFERA ha cumplido con sus obligaciones de medios y ha actuado de forma diligente en todo momento.

4.2. De la improcedencia de interpretar las medidas reactivas como insuficiencia preventiva.

Alega que la capacidad de una empresa para aprender de un incidente y ajustar sus mecanismos de protección es precisamente lo que garantiza una mayor seguridad para los datos de los clientes en el futuro. Considera que penalizarla por ello, evidencia una dinámica donde, desde una perspectiva enfocada en el resultado, se obvian las medidas implementadas por la mercantil víctima de la brecha de seguridad. Afirma que este proceder es contrario a lo dispuesto en las Directrices 04/2022 del CEPD, según las cuales la cooperación de la empresa, su capacidad para rectificar y mejorar tras un incidente, y su cumplimiento con el principio de responsabilidad proactiva deben influir positivamente en la cuantificación de la sanción final.

De ahí que entienda que las medidas reactivas adoptadas por XFERA no deban ser vistas como un reconocimiento de insuficiencia en las medidas originales, sino como una adaptación lógica y proactiva a las circunstancias derivadas de la brecha.

Y que afirmar que la adopción de medidas de mejora es un reconocimiento de una falta de diligencia previa, llevaría al absurdo de que un responsable del tratamiento no evolucionase su sistema de gestión por temor a que pueda considerarse por esta Agencia como un reconocimiento de una negligencia, lo que provocaría su completa desactualización. Considera que esta concepción es absolutamente errónea y contraria al espíritu de los procesos de mejora continua y el propio RGPD.

De esta forma, expone que el mismo artículo 32 requiere que se lleve a cabo este proceso de evolución de las medidas, requiriendo en su apartado 1.d) que exista: "*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, considera que haber adoptado medidas adicionales no supone ninguna prueba de la inadecuación de las anteriores, constando en el caso que nos ocupa únicamente un incidente aislado, frente a los millones de procedimientos realizados por esta entidad en la que ha quedado acreditada la eficacia de las medidas.

QUINTA. - DE LA INADMISIÓN DE LA RESPONSABILIDAD OBJETIVA.

Alega que la AEPD en su Propuesta de Resolución, identifica dos infracciones, con base, exclusivamente, en un escueto análisis del resultado, considerando que la concurrencia de una brecha de seguridad conlleva la automática consideración de que no se adoptaron medidas adecuadas y, por tanto, a juicio de la AEPD, surgiendo automáticamente la responsabilidad directa por parte de XFERA.

Considera que la AEPD establece así una obligación de resultado, sin entrar a valorar el tratamiento de datos personales efectivamente realizado. Afirma que la imputación de dos infracciones muy graves, con la imposición de la consiguiente sanción, fundamentada exclusivamente en un resultado indeseado en un supuesto aislado supone adoptar un principio de responsabilidad objetiva en el ámbito sancionador, vetado por nuestro ordenamiento jurídico.

Expone que la AEPD parece confundir el concepto de responsabilidad proactiva con la obligación de resultado que impone la responsabilidad objetiva, independientemente de si media dolo o culpa por parte de XFERA.

Concluye que al no haberse acreditado la concurrencia de una actuación culpable, intencionada o negligente por parte de XFERA no procede la identificación de la conducta en una infracción de la normativa de protección de datos personales por el mero hecho de haber sido víctima de un acto delictivo y, consecuentemente, no procede la imposición de ningún tipo de sanción.

Considera que la presente Propuesta de Resolución no es ajustada a derecho, pues impone a XFERA una obligación de resultado, consistente en el establecimiento de medidas infalibles, al imputar una infracción del artículo 5.1 apartado f) y del artículo 32 del RGPD basándose únicamente en el resultado que se produce por la actuación criminal de un tercero, sin atender a la diligencia utilizada y sin considerar el despliegue de medidas técnicamente adecuadas e implantadas.

En el caso que nos ocupa, afirma que no hay indicios de que la empresa actuara de forma negligente. Considera que la información obrante en el expediente muestra lo contrario: XFERA implementó medidas preventivas razonables, como la monitorización constante de sus sistemas, lo que permitió detectar el acceso irregular. Expone que el incidente de seguridad se produjo debido a una operación técnica sobre la configuración del DNS, que permitía el acceso evitando el proxy de autenticación de VFR y que, por tanto, este fallo técnico no puede considerarse negligente, ya que se trató de un incidente aislado puntual (fruto de unos trabajos en curso) y no de una falta sistemática de seguridad. Además, añade que, tras la detección de la brecha, XFERA actuó con celeridad para mitigar los daños, notificando a la AEPD y a los afectados dentro de los plazos establecidos y adoptando medidas adicionales para reforzar su sistema de seguridad.

Incide en que la actuación de XFERA tras el incidente demuestra un esfuerzo constante por minimizar los riesgos y proteger los derechos de los interesados.

Por todo lo anterior, considera que la Propuesta de Resolución no resulta conforme a derecho, al imponer a XFERA una responsabilidad objetiva, consistente en la exigencia de adopción de unas medidas infalibles, no admisible por nuestro ordenamiento jurídico.

SEXTA. - SOBRE LA EXISTENCIA DE UN CONCURSO MEDIAL.

Insiste en que ante una sola acción ilícita que ha sido calificada con dos infracciones distintas, se infringe el principio non bis in ídem, consagrado en el artículo 31.1 de la Ley 40/2015.

Afirma que no existe esa supuesta diferencia entre que un artículo se refiera a la infracción de la obligación de confidencialidad y otro a la adopción de medidas adecuadas, sino que ambos se refieren a la aplicación de medidas técnicas u organizativas apropiadas para garantizar la seguridad en el tratamiento de los datos.

Considera que ambas infracciones se proyectan sobre una única conducta supuestamente infractora —la omisión o insuficiencia de medidas técnicas y organizativas adecuadas para proteger los datos personales—, cuya consecuencia directa es la pérdida de confidencialidad. No se trata, por tanto, en su opinión, de dos acciones diferenciadas que pudieran justificar sanciones autónomas, sino de una única acción con una única finalidad vulnerada: la seguridad de los datos personales.

Solicita a la Agencia que, en aplicación de los principios de non bis in ídem, ante la concurrencia de un concurso medial o concurso de infracciones, proceda a calificar los hechos imputados exclusivamente como infracción del artículo 5.1 f) del RGPD, en la medida en la que es la infracción que se identifica como más grave, descartando la aplicación adicional del artículo 32 del RGPD, dejando ésta última sin efectos.

SÉPTIMA. - SOBRE LA FALTA DE PROPORCIONALIDAD DE LA SANCIÓN.

Ratificándose en las previas alegaciones al Acuerdo de Inicio, considera que, habiendo sido XFERA. diligente en su actuación, no procede la imposición de sanción alguna. No obstante, para el hipotético caso de que se considerase la existencia de un supuesto incumplimiento de la normativa de protección de datos, considera que la sanción que pretende imponer la AEPD no resulta, en ningún caso, proporcional, tanto por su cuantía desproporcionada como por la aplicación incorrecta de los elementos moduladores de la responsabilidad

Expone que la AEPD, al imponer una sanción tan elevada en el presente caso, parece pasar por alto el esfuerzo realizado por XFERA para minimizar los daños y reforzar sus medidas de seguridad tras la brecha. Este tipo de actuación debería ser valorada positivamente, en lugar de considerar la sanción como un mero castigo por la ocurrencia del incidente e, incluso, tratar de agravarlo por la adopción diligente de medidas complementarias.

7.1. Sobre la supuesta infracción del artículo 5.1.f) RGPD.

7.1.1 Agravantes invocados por la AEPD.

Sobre "*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 perjuicio que hayan sufrido*"

Afirma que, de los ***CANTIDAD.3 notificados por la brecha de seguridad, solo ocho personas formularon reclamaciones y que, de dichas reclamaciones, ninguna acredita perjuicio económico o uso ilícito de los datos.

En su opinión, la inexistencia de reclamaciones acreditativas de perjuicios concretos, la ausencia de vínculo causal con la brecha en los pocos casos que alegan afectación, y el carácter meramente especulativo de los daños invocados, desacreditan objetivamente la pretensión de agravar la infracción con base en unas repercusiones para los interesados que, en la práctica, no se han materializado.

La intencionalidad o negligencia en la infracción.

Considera que no resulta acreditado que XFERA haya incurrido en una falta de diligencia sancionable, y menos aún que tal conducta pueda ser calificada de grave. Lejos de ello, afirma que los hechos muestran una actuación proporcionada, técnica y organizativamente coherente, que excluye toda intencionalidad o negligencia grave. Por ello, considera que resulta improcedente aplicar la circunstancia agravante.

Sobre las categorías de los datos de carácter personal afectados por la infracción.

Alega que la aplicación del agravante del artículo 83.2.g) RGPD carece de base jurídica y fáctica, incurre en duplicidad sancionadora y constituye una extensión indebida de un precepto que debe reservarse a supuestos de tratamiento de datos especialmente sensibles. En consecuencia, solicita que se elimine dicha circunstancia de la valoración agravatoria de la infracción.

Sobre toda infracción anterior cometida por el responsable o el encargado del tratamiento.

Expone que la AEPD sostiene que deben considerarse como agravantes las resoluciones sancionadoras dictadas en procedimientos anteriores contra esa entidad, concretamente los expedientes PS/00027/2021, PS/00448/2020 y PS/00104/2020. Sin embargo, afirma que esta apreciación resulta improcedente por varias razones que afectan tanto a su relevancia jurídica como a su adecuación fáctica al caso que nos ocupa.

En primer término, porque las resoluciones PS/00448/2020 y PS/00104/2020 hacen referencia a hechos ocurridos en los años 2019 y 2020 y en segundo lugar porque la propia lógica del sistema sancionador exige un mínimo de actualidad en la conducta precedente para ser valorada como indicio de reincidencia o tendencia.

Afirma que atribuirles dicho valor resultaría, en la práctica, improcedente, en la medida en la que no guardan vinculación con el presente supuesto de hecho.

Sobre la vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

Considera que no concurre la circunstancia agravante prevista en el artículo 76.2.b) LOPDGDD, ya que:

• No existe una relación directa entre el tratamiento ordinario de datos personales por parte de XFERA y el incidente objeto del procedimiento.
• El hecho generador de la brecha es una acción delictiva externa que convierte a esta entidad en sujeto pasivo de una conducta ajena.
• La aplicación automática del agravante desnaturaliza su finalidad y vulnera el principio de proporcionalidad y de tipicidad sancionadora.

7.2 Sobre la supuesta Infracción del artículo 32 RGPD.
7.2.1 Agravantes invocados por la AEPD.

Sobre 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.

Reitera que la entidad ha cumplido diligentemente con dicho mandato, adoptando medidas conforme al principio de responsabilidad proactiva del artículo 24 RGPD, incluyendo protocolos de respuesta rápida, notificación oportuna y colaboración plena con la autoridad de control.

Considera que el incidente de seguridad fue causado por agentes externos maliciosos, no por una actuación negligente o deliberada de esta entidad, lo que refuerza que no existió una cesión o uso ilícito de los datos por parte del responsable, sino una conducta ilícita de terceros frente a la cual se actuó con la diligencia debida.

Alega que no consta en el expediente perjuicio alguno acreditado, ni material ni inmaterial, sufrido por los interesados afectados, lo cual impide considerar que se haya producido una afectación real, efectiva y concreta del derecho fundamental, más allá de un riesgo hipotético que fue gestionado y mitigado por esta entidad conforme a los estándares del RGPD.

Sobre la intencionalidad o negligencia en la infracción.

Considera que se ignoran por completo los límites técnicos razonables de cualquier sistema de seguridad, así como el marco legal aplicable, que no exige una invulnerabilidad absoluta, sino un despliegue proporcionado de medidas ajustadas al riesgo.

En esencia, insiste en que la brecha no fue consecuencia de una omisión deliberada o de una ausencia de medios, sino de un encadenamiento excepcional de factores que no podía preverse razonablemente, incluso en escenarios de gestión avanzada del riesgo. En cualquier caso, como ya ha señalado, manifiesta que la ausencia de consecuencias reales debería llevar a una valoración más prudente de la gravedad del incidente, especialmente cuando la entidad afectada adoptó de forma inmediata medidas de contención, notificó a la Agencia y a los interesados, y revisó de forma exhaustiva sus sistemas para prevenir futuras incidencias.

Sobre toda infracción anterior cometida por el responsable o el encargado del tratamiento.

Expone que el expediente no aporta elementos propios ni diferenciados que permitan sostener una agravación específica en el contexto del artículo 32, más allá de lo ya alegado de forma general sobre la supuesta falta de diligencia. Por tanto, considera que mantener la agravación en este apartado con base en una justificación genérica y ya replicada implica una vulneración del principio de motivación suficiente y no reiterativa en el ejercicio de la potestad sancionadora.

En consecuencia, entiende que no procede aplicar la agravante del artículo 83.2.b) RGPD en relación con la presunta infracción del artículo 32, por tratarse de una

valoración idéntica a la ya impugnada y por no aportar la AEPD justificación adicional ni específica que sustente su aplicación diferenciada en este contexto.

Sobre la vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

Alega que la AEPD reitera la aplicación del agravante relativo a la vinculación de la actividad del responsable con el tratamiento de datos personales, esta vez en el contexto del artículo 32 RGPD, sin introducir elementos nuevos que justifiquen su aplicación diferenciada. Afirma que esta duplicidad incurre en una valoración reiterativa que, en la práctica, multiplica el efecto sancionador a partir de una misma base fáctica, lo que resulta contrario al principio de proporcionalidad.

Además, tal y como ha argumentado a lo largo del presente procedimiento, en el presente supuesto, entiende que la existencia de una brecha de seguridad provocada por un ataque externo no guarda relación directa con la actividad comercial ordinaria de XFERA ni con la forma en que esta trata los datos en su operativa diaria. Insiste en que la actividad de tratamiento no fue origen ni causa del incidente, y menos aún un factor agravante del mismo. Considera que aplicar el agravante sobre esta base desvirtúa su finalidad y genera un efecto automático que vacía de contenido su valoración casuística.

Sobre las atenuantes no apreciadas por la Agencia.

Expone que, conforme al principio de proporcionalidad sancionadora, resulta imprescindible que, junto a la gravedad de los hechos, se valoren también todas las circunstancias atenuantes que concurran en el caso, volviéndolas a invocar.

1) Medidas correctoras adoptadas para mitigar las consecuencias de la brecha (art. 83.2.c RGPD)
2) No afectación de categorías especiales de datos personales (art. 83.2.g RGPD)

3) Cooperación activa con la Agencia Española de Protección de Datos (art. 83.2.f RGPD)

4) Adhesión a códigos de conducta y mecanismos de certificación (art. 83.2.j RGPD)

Alega que la compañía cuenta con certificaciones reconocidas internacionalmente, aprobados con arreglo al artículo 42, tales como la ISO 27001, de Sistema de Gestión de Seguridad de la Información; e ISO 27701, de Gestión de la Privacidad de la Información; cuyas evidencias se aportan como Documento n.º 8 y Documento n.º 9, respectivamente. Asimismo, se aporta el certificado, como Documento n.º 10, correspondiente a la certificación del Esquema Nacional de Seguridad nivel Alto de XFERA.

Además, afirma que XFERA se encuentra entre los operadores de telecomunicaciones que suscribieron con AUTOCONTROL sendos Códigos de Conducta, conforme al artículo 40 del RGPD, uno de Tratamiento de Datos en la actividad publicitaria (Documento n.º 11) y otro para la resolución de controversias de protección de datos en el sector de las comunicaciones electrónicas (Documento n.º 12).

5) Inexistencia de beneficio económico derivado del incidente (art. 83.2.k RGPD)

Por último, solicita la apertura del periodo probatorio en el que sean admitidos y practicados los siguientes medios de prueba:

• Pericial, a realizar por ***J.J.J. y L.L.L.***, ambos Profesores titulares de la Universidad de ******LOCALIDAD.1***, y cuyo ámbito, detallado en la Carta de aceptación de encargo que se anexa como Documento n.º 13, se referirá al análisis de las medidas de seguridad de XFERA que pudiesen ser de interés en relación con este procedimiento. Indica que este informe está siendo redactado en la actualidad, y será aportado a esta digna Agencia a la mayor brevedad, al amparo de lo previsto en el artículo 76.1 de la LPAC.

Por todo lo expuesto, solicita a la AEPD que tenga por formuladas las anteriores alegaciones, por aportados los documentos que se facilitan y por propuestos los indicados medios de prueba y previos los trámites oportunos:

I. Dicte resolución por medio de la cual señale el archivo del Procedimiento n.º 07113/2023, con base en la existencia de un procedimiento penal en curso que afecta de forma sustancial a los hechos probados sobre los que versa el presente expediente.

II. Subsidiariamente, dicte resolución por medio de la cual señale el archivo del Procedimiento n.º 07113/2023, debido a ausencia de culpa o negligencia de XFERA.

III. Subsidiariamente a todo lo anterior, en el caso de que la AEPD resuelva en contra de la fundamentación jurídica que sostiene XFERA, solicita a la AEPD que tenga en cuenta las circunstancias atenuantes fundamentadas en las anteriores alegaciones y, consecuentemente, culmine el procedimiento mediante un apercibimiento y, en última instancia, si considera que procede la imposición de una sanción, modere o module la recogida en la Propuesta de Resolución, atendiendo a los argumentos manifestados en el cuerpo del presente escrito de alegaciones.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: ***A.A.A.***, ***B.B.B., C.C.C., D.D.D., E.E.E., F.F.F., G.G.G.*** y ***H.H.H.,*** interpusieron reclamaciones ante la Agencia Española de Protección de Datos, contra XFERA MÓVILES, S.A.U., con NIF A82528548.

Los motivos en que basan sus reclamaciones son los siguientes:

Reclamación 1, fecha de entrada 2 de abril de 2023 y registro REGAGE23e00021932536, con los siguientes datos asociados:

- Reclamante: ***A.A.A.***
- Reclamado: XFERA

- Hechos según manifestaciones de la parte reclamante:" He *recibido correo del proveedor de telefonía indicando que terceras personas han accedido a datos personales con el objeto de suplantación de identidad, razón por la cual, quiero interponer demanda, ya que no han garantizado la seguridad e integridad de la información personal que se les ha suministrado.*"
- Aporta captura con correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 1 de abril de 2023 con información sobre un incidente de seguridad que afectó a sus datos personales.

Reclamación 2, fecha de entrada 8 de abril de 2023 y registro REGAGE23e00022985593, con los siguientes datos:

- Reclamante: ***B.B.B.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Brecha de seguridad en la base de datos de clientes de Yoigo; terceras personas se han hecho con datos personales míos, sin mi autorización, con el riesgo que conlleva. Dicha posible brecha se me informo ayer 07/04/2023 por correo electrónico y se me ha confirmado hoy día 8 de abril mediante llamada telefónica al número ***TELÉFONO.2, número que se me indicaba en el correo y que me han confirmado por Twitter, de Yoigo donde se me ha indicado que los datos sustraídos son, como mínimo, mi nombre, número de identificación, teléfono y número de cuenta bancaria*".
- Aporta captura de pantalla con la información recibida por parte de Yoigo comunicando el incidente de seguridad.

Reclamación 3, fecha de entrada 10 de abril de 2023 y registro REGAGE23e00023162950, con los siguientes datos:

- Reclamante: ***C.C.C.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *YOIGO remitió a sus clientes un correo electrónico informativo con fecha 6 de abril de 2023, a las 14:07 horas, en el que se nos comunicaba tales circunstancias (correo que adjunto al presente escrito), y que pude constatar al contactar con el servicio de atención al cliente de la operadora en la que confirman que mis datos se han visto afectados, desde el nombre y dirección, hasta el DNI o el número de la cuenta corriente.* "
- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 6 de abril de 2023 comunicando el incidente de seguridad y la afectación de sus datos personales."

Reclamación 4, con fecha de entrada 10 de abril de 2023 y registro REGAGE23e00023074494, con los siguientes datos:

- Reclamante: ***D.D.D.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *En el mes de marzo se me ha añadido un coste en la factura del teléfono de 1.99. Al contactar con Yoigo me dicen que no saben de donde procede y que lo único que saben es*

*que se dado de alta en tienda física de Yoigo. Me dan un teléfono (*****TELÉFONO.1**) para que pueda aclarar importe. Es una empresa que protección de datos, pero yo no he contratado. Tampoco me dicen de donde ha salido el alta. Me informan que puedo enviar correo para dar de baja. (*****EMAIL.2**) para dar de baja una póliza que nunca he contratado. El importe no me lo devolverán. Días más tarde recibo mail de Yoigo donde especifica que 'debemos ponernos en contacto contigo para informarte que hemos experimentado un incidente, por el cual terceras personas ajanes a nuestra organización pueden haber accedido a algunos de tus datos personales...'*

- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 6 de abril de 2023 con la información sobre el incidente de seguridad y la afectación de datos personales."

Reclamación 5, con fecha de entrada 23 de abril de 2023 y registro REGAGE23e00025932054, con los siguientes datos asociados:

- Reclamante: ***E.E.E.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Me dirijo a ustedes con relación al robo de datos personales que ha sufrido mi compañía telefónica, XFERA MOVILES SAU, con nombre comercial YOIGO.A pesar de ser uno de sus clientes, no he recibido ninguna información sobre qué datos míos se han visto comprometidos. Por tanto, me gustaría hacer una reclamación por el tratamiento de mis datos personales. Solicito que se me informe qué datos míos se han visto comprometidos y cómo se han visto afectados, teniendo en cuenta que también se pueden haber visto comprometidos los datos de las líneas de las que soy titular siendo 3 líneas móviles y 1 línea fija. Además, solicito que se tomen las medidas necesarias para garantizar que esto no vuelva a suceder. Asimismo, considero que he sufrido daños y perjuicios como resultado de este incidente y solicito que se me indemnice adecuadamente por ello, teniendo en cuenta además como he indicado anteriormente que soy titular de 4 líneas telefónicas en la compañía y se pueden haber visto comprometida también información de las mismas.* "
- Aporta:
  - Captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 6 de abril de 2023 con la información sobre el incidente de seguridad y la afectación de datos personales.
  - Copia de DNI, copia del contrato con la compañía y factura de servicios.

Reclamación 6, con fecha de entrada 23 de abril de 2023 y registro REGAGE23e00026221929, con los siguientes datos asociados:

- Reclamante: ***F.F.F.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *Debido al ciberataque sufrido por Yoigo a principios de marzo, me informan que mis datos PERSONALES podrían haber sido expuesto (nombre, apellidos, números de teléfono, DNI, CUENTA BANCARIA, etc.) a ciberdelincuentes. Debido a esto, desde hace 2-3 semanas he recibido phishing muy sofisticado, pero eso no es lo grave. Lo grave, es que mi cuenta bancaria corresponde a un banco vasco*

muy pequeño, y debido a que les han sustraído mis datos, los ciberdelincuentes saben perfectamente a que banco corresponde mi cuenta bancaria (por el IBAN). Por este motivo, el phishing que estoy recibiendo a todas horas, no solo es sofisticado, sino que está totalmente teledirigido a mi porque conocen todos los datos que arriba menciono. Estoy tremendamente afectado y con el temor de cualquier día caer en la trampa, porque he visto mucho phishing, pero este es muy sofisticado. Como cliente de Yoigo, me veo tremendamente perjudicado y gracias a a esta empresa, vivo con la angustia de caer en alguna trampa y perder mi patrimonio. La presente reclamación es debido a que Yoigo no ha hecho una correcta custodia de mis datos personales y esto me está provocando graves daños psicológicos por las razones antes expuestas. Es curioso, que, dentro de mi contrato, hay 3 líneas más, pero la única que recibe el phishing soy yo, porque soy el titular del contrato y de la cuenta bancaria. Es una evidencia, que este ataque no responde al azar. "

- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 5 de abril de 2023 con la información sobre el incidente de seguridad y la afectación de datos personales.

Reclamación 7, con fecha de entrada 11 de mayo de 2023 y registro REGAGE23e00030222022, con los siguientes datos asociados:

- Reclamante: ***G.G.G.***
- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" *El día 2 de abril de 2023, recibo un mail de dicha empresa Yoigo que aporto como prueba documental adjunta al presente escrito, en virtud de la cual, se me pone en conocimiento de la existencia de un ciberataque en la citada empresa, lo que ha motivado que mis datos personales tanto propios como los de mi familia que figurasen almacenados pudieran haber quedado expuestos frente a terceros de forma indebida. Tras llamar al número de teléfono que figura en el mail no me facilitaron más información que la que ya consta en el mail aportado (no concretando qué datos en particular serían o si ha sido en grado de tentativa o efectivamente se ha consumado una intromisión indebida, y por supuesto tampoco admiten ninguna reparación o indemnización por ello al cliente). Desde dicha fecha vengo recibiendo mensajes fraudulentos como por ejemplo un mail manifestando que tengo un paquete esperando, o algunos SMS suplantando mi Banco manifestando que tengo un problema en mi cuenta, lo que claramente se infiere que se trata de mensajes fraudulentos o phishing. El perjuicio consistente en que puedan suplantarme o el temor a un potencial futuro uso indebido de sus datos personales, cuya existencia haya sido demostrada por el interesado, puede constituir un daño moral que genere derecho a indemnización* "
- Aporta captura de pantalla de correo electrónico recibido desde la dirección ******EMAIL.1*** en fecha 2 de abril de 2023 con la información sobre el incidente de seguridad y afectación de datos personales.

Reclamación 8, con fecha de entrada 30 de mayo de 2023 y registro REGAGE23e00034386550, con los siguientes datos asociados:

- Reclamante: ***H.H.H.***

- Reclamado: XFERA
- Hechos según manifestaciones de la parte reclamante:" Soy *cliente de Yoigo. En abril recibí un mail en el que se me comunicaba que TODOS los datos de los clientes habían sido filtrados. Solicité que me dijeran explícitamente qué datos. Este grupo ha infringido el RGPR y la LOPDGDD al no custodiar debidamente la información requerida para contratar sus servicios y desde ahora mi identidad puede ser manipulada para fines ilícitos y por tiempo indeterminado. Me gustaría acogerme al amparo de la AEPD ya que esta filtración supone una situación de vulnerabilidad personal crítica por las incorrectas medidas de seguridad tomadas por la empresa Yoigo-GRUPO MASMOVIL - XFERA MOVILES, S.A.U.* "
- Aporta:
    - Captura de pantalla del correo inicial recibido desde la dirección ******EMAIL.1*** en fecha 3 de abril de 2023 con información sobre el incidente de seguridad y afectación de datos personales.
    - Captura de pantalla de correo enviado por el reclamante a la dirección ******EMAIL.3*** solicitando información adicional sobre el incidente.
    - Captura de pantalla de correo de respuesta recibido desde la dirección ******EMAIL.3*** con el siguiente contenido:

      "*En relación con el incidente, le informamos que hemos detectado un acceso no autorizado a una de las aplicaciones que dan soporte a nuestro canal presencial que permite la visualización de ciertos datos, como datos identificativos, de contacto, información de los servicios contratados con nosotros y el IBAN.*
      Como indicábamos en la comunicación, es posible que estos datos sean utilizados para intentar usurpar su personalidad, principalmente ante nosotros, si bien hemos modificado nuestras políticas para evitar dicha circunstancia. También le informamos que solo con la información accedida no debería ser posible, por ejemplo, contratar ningún servicio (puesto que requiere de un mandato SEPA) ni acceder a su cuenta bancaria.
      En todo caso, le recomendamos que tenga cuidado con correos electrónicos, SMS o llamadas que pueda recibir de remitentes desconocidos o que no se identifiquen claramente, en especial si le solicitan códigos, claves de acceso o datos de tarjeta de crédito.
      *En caso de que detecte cualquier actividad sospechosa, le recomendamos que se ponga en contacto con su entidad bancaria y denuncie los hechos a la policía. También puede ponerse en contacto con el Instituto Nacional de Ciberseguridad (INCIBE) en el número 017 o consultar su sitio web ***URL.1.*
      Esperamos haber resuelto sus cuestiones, en cualquier caso, estamos a su disposición"

SEGUNDO: Previamente a estas reclamaciones, el 31 de marzo de 2023, XFERA se puso en contacto con la AEPD para realizar la notificación de la quiebra de seguridad de datos personales relacionada con las reclamaciones anteriores. Con fecha 28 de abril de 2023 y registro de entrada REGAGE23e00027432375, XFERA amplió la información sobre la quiebra. De su contenido se extrae la siguiente información relevante:

- *Los datos no estaban cifrados, anonimizados o protegidos de forma ininteligible.*
- *Descripción de la brecha:* "*(…).*"

- Número aproximado de personas físicas sobre las que se realizan operaciones de tratamiento referidas al tratamiento sobre el que se ha producido la brecha de datos personales: ***CANTIDAD.1
- Afectados ***CANTIDAD.2
- Fecha de detección de la brecha: 28/03/2023
- Fecha de inicio de la brecha: 05/03/2023
- Fecha en la que se dio por resuelta la brecha: 03/04/2023
- Se comunicó a ***CANTIDAD.3.
- Fecha en la que se informó: 10/04/2023

TERCERO: En relación con el vector de entrada de la brecha, ha quedado constatado que (…).

En fecha 19 de abril de 2023, XFERA procedió a presentar una denuncia en relación con los hechos que propiciaron la brecha ante el Cuerpo Nacional de Policía, ***(…)***.

CUARTO: (…)

QUINTO: Ha quedado constatado que la brecha afectó a un volumen aproximado de ***CANTIDAD.4 de la entidad, filtrándose la siguiente tipología de datos personales: Nombre y apellidos, fecha de nacimiento, número de NIF, correo electrónico, números de teléfono, IBAN de la cuenta asociada y dirección física.

El IBAN de la cuenta asociada se encontraba sin cifrar ni anonimizar, como se desprende de la notificación de brecha realizada por XFERA, con registro de entrada REGAGE23e00027432375, en la que consta:

"Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?

No"

El dato del IBAN, que se mostraba en VRF antes de la brecha, era utilizado por XFERA, según ha informado a esta Agencia, no para autenticar al cliente, sino para procesos de negocio que requerían que se informase al cliente del número de cuenta en el que se estaba cargando la factura al mismo.

SEXTO: Entre las medidas reactivas se ha constatado:

- ***(…)***

SÉPTIMO: Entre las medidas preventivas ha quedado constatado:

- ***(…)***

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 resolver este procedimiento, la Presidencia 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

XFERA MÓVILES S.A. es una gran empresa del sector de las telecomunicaciones que ofrece servicios de telefonía fija, telefonía móvil, internet (fibra y 5G) y televisión (Agile TV) en España.

Para ello trata datos de carácter personal, entendiendo por dato de carácter personal: *"toda información sobre una persona física identificada o identificable*".

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

«responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.*

Se considera persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Asimismo, debe entenderse por tratamiento "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

El artículo 4 apartado 12 del RGPD define, *«violación de la seguridad de los datos personales»: como 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.*

En el presente caso, consta una notificación inicial de brecha de datos personales presentada, en fecha 31 de marzo de 2023, ante esta Agencia por parte de XFERA MOVILES SAU, y que está relacionada con las reclamaciones anteriores, y una notificación posterior, efectuada en fecha 28 de abril de 2023.

En cuanto a la tipología de datos personales que fueron filtrados destacan: nombre y apellidos, fecha de nacimiento, número de NIF, correo electrónico, números de teléfono, IBAN de la cuenta asociada y dirección física. Los datos no estaban cifrados, anonimizados o protegidos de forma ininteligible.

(…).

Consta que en fecha 19 de abril de 2023, Xfera procedió a presentar una denuncia en relación con los hechos que propiciaron la brecha ante el Cuerpo Nacional de Policía, ***(…).***

(…).

En este caso, la pronta actuación de la Policía Nacional ha propiciado ***(…)***. Xfera afirma mantener las medidas implantadas para mitigar los riesgos de los interesados afectados (cambio en políticas de identificación/autenticación de clientes, vigilancia de la Deep Web y vigilancia estadística de patrones anómalos en clientes) mientras no tenga constancia de que no hay ya riesgos para los clientes afectados.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD.

Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control y la comunicación de una violación de la seguridad de los datos personales al interesado, respectivamente.

De las actuaciones de investigación desarrolladas por la presenta autoridad, XFERA afirma, en relación con la infracción del artículo 34 del RGPD, que en fecha 31 de marzo de 2023, se inició el proceso de comunicación de la violación de la seguridad de los datos personales a los interesados. Esta comunicación se realizó individualmente a cada uno de los afectados por el ataque, al tener XFERA los logs (registros técnicos) que permitían saber cuáles de sus clientes habían sido afectados por el ataque y cuáles no. Para ello se utilizó prioritariamente la vía del correo electrónico, y como alternativa, el SMS para aquellos casos en los que el cliente no había aportado un correo electrónico como dato de contacto, o hubo problemas en el envío.

III

Alegaciones al Acuerdo de inicio

En relación con las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto:

PRIMERA. Necesaria suspensión del procedimiento por prejudicialidad penal.

XFERA alega que los hechos objeto de este procedimiento sancionador se encuentran bajo investigación penal, como consecuencia de la denuncia presentada; investigación que ha recaído en el Juzgado de Instrucción n.º 28 de Madrid y está siendo sustanciada a través de las ******DILIGENCIAS.1***, en las que Xfera se ha personado como acusación particular.

En este caso, considera que nos encontramos ante una situación en la que los mismos hechos están siendo investigados en sede penal, y donde cualquier decisión administrativa prematura podría resultar contradictoria con lo que se resuelva en tal jurisdicción. Por ello, entiende que, en aplicación del principio de prejudicialidad penal, no debe resolverse el asunto en vía administrativa en tanto en cuanto no se resuelva por la vía penal dado que en este procedimiento concurren la triple identidad de sujeto, hecho y fundamento que exige la jurisprudencia para suspender la tramitación de un procedimiento sancionador por prejudicialidad penal.

A este respecto, debe tenerse en cuenta que el artículo 77.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas dispone que:

"*En los procedimientos de carácter sancionador, los hechos declarados probados por resoluciones judiciales penales firmes vincularán a las Administraciones Públicas respecto de los procedimientos sancionadores que substancien*".

En relación con esta cuestión, esta Agencia considera necesario señalar que, en el presente expediente sancionador no existe la triple identidad necesaria para aplicar el artículo 77.4 de la Ley 39/2015, de sujeto, hecho y fundamento entre la infracción administrativa que se valora y la posible o posibles infracciones penales que se pudieran derivar de la denuncia presentada ante el órgano jurisdiccional, en la medida en que el sujeto infractor no es el mismo.

De este modo, XFERA, con NIF A82528548, es el sujeto responsable en el presente procedimiento sancionador, mientras que el responsable penal de un presunto delito de estafa sería un tercero. Aspecto que XFERA no ignora pues ha esgrimido con insistencia en sus alegaciones al acuerdo de inicio, como un argumento a su favor, su condición de "*víctima de una actuación criminal".*

Tampoco el fundamento jurídico sería el mismo: mientras el bien jurídico protegido por la LOPDGDD, es el derecho fundamental a la protección de datos personales, el bien jurídico que se protege en el tipo penal de estafa, cuya comisión investiga el Juzgado de Instrucción n.º 28 de Madrid, es el patrimonio ajeno.

En este sentido es muy esclarecedora la Sentencia de la Audiencia Nacional de 27/04/2012 (rec. 78/2010), en cuyo Fundamento Jurídico segundo el Tribunal se pronuncia en los siguiente términos frente al alegato de la recurrente de que la AEPD ha infringido el artículo 7 del R.D. 1398/1993 (norma que estuvo vigente hasta la entrada en vigor de la LPACAP): "*En este sentido el Art. 7 del Real Decreto 1398/1993, de 4 de agosto, del procedimiento para el ejercicio de la potestad sancionadora, únicamente prevé la suspensión del procedimiento administrativo cuando se verifique la existencia efectiva y real de un procedimiento penal, si se estima que concurre identidad de sujeto, hecho y fundamento de derecho entre la infracción administrativa y la infracción penal que pudiera corresponder.*

No obstante, y para la concurrencia de una prejudicialidad penal, se requiere que ésta condicione directamente la decisión que haya de tomarse o que sea imprescindible para resolver, presupuestos que no concurren en el caso examinado, en el que existe una separación entre los hechos por los que se sanciona en la resolución ahora recurrida y los que la recurrente invoca como posibles ilícitos penales. Así, y aun de haberse iniciado, en el presente supuesto, y por los hechos ahora controvertidos, también actuaciones penales frente a la empresa distribuidora, lo cierto es que tanto la conducta sancionadora como el bien jurídico protegido son distintos en una y otra vía (contencioso-administrativa y penal). En el ámbito penal, el bien jurídico protegido es una posible falsedad documental y estafa, y en el ámbito administrativo, en cambio, la facultad de disposición de sus datos personales por parte de su titular, por lo que tal objeción de la demandada ha de ser rechazada".

Por tanto, la cuestión planteada por Xfera no puede prosperar y debe ser rechazada.

SEGUNDA. - SOBRE EL SUPUESTO DE HECHO

Del examen de los hechos relativos al incidente de seguridad, afirma que la Agencia identifica como constitutivo de infracción, el mero hecho de que se produzca una brecha de seguridad y que se hayan presentado reclamaciones por quienes fueron diligentemente informados de la misma, siendo éste último hecho el único que, en su opinión, hace que la AEPD vuelva a reactivar un procedimiento, respecto al que ella misma había dictado que "*no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales"*, sin que se atienda, ni analice el concreto supuesto de hecho, la ausencia de perjuicio asociado o de publicación en abierto de los datos, las medidas de seguridad implementadas, ni las responsabilidades derivadas.

A este respecto, debe tenerse en cuanta que, en el encabezado del escrito de 12 de mayo de 2023, citado por XFERA, consta *"DIVISIÓN DE INNOVACIÓN TECNOLÓGICA*" y finaliza indicando que "*no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales*."

Por tanto, en contra de lo que afirma la entidad investigada, este escrito no tiene carácter decisorio, ni por su contenido (más bien es un "acuse de recibo" de la brecha notificada) que se encuentra circunscrito al acto de la notificación y a las posibles acciones de la División, y que en modo alguno puede entenderse como si esta AEPD hubiese valorado que no concurría 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 la entidad, ni tampoco por su forma, pues ni siquiera formalmente refleja una decisión en tal sentido, ni mucho menos una resolución de archivo de actuación alguna, pues para que ello sea así, sería necesario que tales actuaciones se hubiesen iniciado.

Dicho escrito está encaminado a poner en conocimiento de XFERA la recepción de la notificación de la brecha acaecida y de su incorporación al registro de notificaciones de brechas, de acuerdo con lo determinado en el artículo 31.d) del Estatuto de la Agencia, aprobado mediante Real Decreto 389/2021, de 1 de junio, sin que pueda deducirse a la vista del mismo, que la AEPD valoró y decidió que no concurría responsabilidad alguna por un supuesto incumplimiento de la normativa de protección de datos. Únicamente informa que por la DIT no se prevé realizar más actuaciones relacionadas con el acto de comunicación de la brecha, pero todo ello sin perjuicio de que puedan iniciarse otras actuaciones, como resulta obvio.

Así, el artículo 13 del Estatuto de la AEPD 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.

El artículo 57, Funciones, del RGPD en su letra h) establece que:

"1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

(…)

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particu-lar basándose en información recibida de otra autoridad de control u otra autoridad pú-blica;

(…)

En cuanto a las funciones de la Subdirección General de Inspección de Datos de la AEPD, el artículo 27 del Estatuto de la Agencia indica, en su apartado 1, que:

"La Subdirección General de Inspección de Datos es el órgano administrativo, depen-diente 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 ci-tado Reglamento"

Y en el apartado 2 de este artículo 27 enumera las funciones que corresponden a la Subdirección General de Inspección de Datos de Datos, entre las que se encuentran, por lo que aquí interesa, las siguientes:

"a) La supervisión permanente del cumplimiento del Reglamento (UE) 2016/679 del Par-lamento 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 presen-tada ante la Agencia Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 77.2 del citado Reglamento.

(…)"

Por tanto, para proceder al archivo de unas actuaciones investigación se requiere, primero, que se hayan iniciado, lo cual no había sucedido en el momento de emitirse el referido escrito de la División de Innovación Tecnológica y, en segundo lugar, es necesaria una resolución expresa por parte de la Presidencia de la Agencia Española de Protección de Datos, 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, se presentaron distintas reclamaciones de clientes a los que la operadora había comunicado el incidente.

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 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

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.

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.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

En relación con las actuaciones previas de investigación el art. 67 de la LOPDGDD dispone lo siguiente:

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 dieciocho 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.

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 la existencia o no 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 concurren los elementos necesarios para la apertura de un procedimiento sancionador. 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, y como indica el artículo 67.2 LOPDGDD referenciado, la AEPD puede llevar a cabo actuaciones previas de investigación. Lo que aconteció en este caso, a fin de lograr una mejor determinación de los hechos y las circunstancias. Es una potestad que tiene atribuida a la AEPD por el RGPD y por la LOPDGDD.

Asimismo, y a mayor abundamiento, incluso en el supuesto de no haber existido las reclamaciones, el escrito cuestionado 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 presentadas en esta AEPD, 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.

A este respecto, se recuerda de nuevo que dichas reclamaciones, sólo se admiten, siendo la documentación y todo lo recopilado durante dichas actuaciones de investigación, lo que ha motivado, exclusivamente, el inicio del presente procedimiento sancionador, y no las citadas reclamaciones.

TERCERA. Vulneración de los principios "non bis in ídem" y de especialidad.

Alega que los hechos que se imputan a Xfera han sido calificados, en el Acuerdo de Inicio, como constitutivos de dos infracciones diferenciadas: por un lado, la vulneración del artículo 5.1.f) del RGPD, tipificada como infracción muy grave, y por otro, el incumplimiento del artículo 32 del RGPD, tipificada como grave.

Considera que el Acuerdo de Inicio explica que la primera sanciona la pérdida de confidencialidad de los datos personales, mientras que la segunda reacciona frente a la insuficiencia de las medidas de seguridad implementadas. Sin embargo, esta calificación resulta, en su opinión, incorrecta, ya que ambas infracciones se aplican sobre una misma conducta y persiguen proteger el mismo bien jurídico, lo que vulnera los dos principios expuestos.

3.1. Vulneración del principio non bis in ídem

Afirma que en el caso que nos ocupa, las dos infracciones propuestas por la Agencia buscan sancionar la misma conducta: la supuesta falta de adopción de medidas técnicas y organizativas suficientes para garantizar la seguridad de los datos personales. No existe, por tanto, en su opinión, una pluralidad de conductas que pueda justificar la doble sanción.

En primer lugar, indicar que los artículos 5.1 f) y 32 del RGPD se tipifican de manera diferenciada en el RGPD. Asimismo, se califican en la LOPDGDD de manera diferenciada, a los efectos de la prescripción, y gozan, cada uno de ellos, de entidad propia.

En el escrito de alegaciones al acuerdo de inicio, XFERA afirma: "*que la conducta sancionada, que es la falta de adopción de medidas de seguridad adecuadas, ha provocado la pérdida de confidencialidad: sin una, no se habría producido la otra. (…) Ambas infracciones, por tanto, derivan de la misma conducta y se relacionan con el mismo bien jurídico, lo que refuerza la idea de que la doble sanción vulnera el principio non bis in ídem.*"

Esta falta de diferenciación entre los hechos sancionados en cada infracción es precisamente lo que le lleva a concluir que se ha vulnerado el principio non bis in ídem.

Pues bien, en relación con las alegaciones que acaban de ser reproducidas, resulta necesario traer a colación la diferencia entre la vulneración del art. 5.1.f) y la del artículo 32 de RGPD, la diferente tipificación en apartados 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 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 e integridad cuando explicita "*mediante la aplicación de medidas técnicas y organizativas apropiadas*", que no son estrictamente de seguridad.

Existen 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 mientras que en el caso del artículo 5.1.f) del RGPD, se debe garantizar la confidencialidad e integridad. Como puede observarse, los dos artículos persiguen fines distintos, 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):
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 que nos ocupa, 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, mientras que 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 esta falta de medidas de seguridad hubiese sido detectada por la AEPD sin que se hubiera producido la pérdida de confidencialidad, únicamente habría sido sancionada por el artículo 32 del RGPD.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de confidencialidad, consecuencia de la deficiente aplicación de medidas técnicas u organizativas apropiadas para garantizar la confidencialidad de los datos y mediante el art. 32 del RGPD la deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento, ajenas a las que habrían posibilitado la materialización de la brecha de datos personales y cuya falta de implantación o de eficacia ha sido conocida por esta Agencia con motivo de la investigación llevada cabo. Estas medidas de seguridad deficientes infringen el RGPD, independientemente de que no se hubiera producido la pérdida de confidencialidad.

Dicho lo anterior, no se comparte el razonamiento expuesto en cuanto a que la AEPD sí ha aplicado este principio (non bis in ídem) en procedimientos como el PS/00027/2021 o el PS/00021/2021, toda vez que, es perfectamente admisible que la

AEPD considere la vulneración de un determinado precepto en el convencimiento de que se ajuste más a los hechos que acontecen, sin que esta actuación pueda considerarse arbitraria, máxime cuando está debidamente motivada. Como ya se ha indicado, 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. Cuando la AEPD decide abrir un expediente sancionador, valora, a la vista de las circunstancias que concurren en el caso concreto, qué infracción o posibles infracciones del RGPD se habrían cometido.

El presente procedimiento sancionador se ha iniciado por la información y documentación obtenida tras el período de actuaciones previas de investigación, al inferirse de las mismas, una posible vulneración a la normativa en materia de protección de datos: el artículo 5.1 f) y el artículo 32 del RGPD.

Por las razones expuestas, no se entiende vulnerado el principio de non bis in ídem.

3.2. Vulneración del principio de especialidad

Alega que el artículo 32 es la norma que se ajusta con mayor precisión a los hechos objeto de este procedimiento, ya que regula de forma detallada las medidas técnicas y organizativas que deben implementarse para garantizar un nivel de seguridad adecuado al riesgo. Y que, por el contrario, el artículo 5.1.f), al ser una disposición más general, debe ceder ante la aplicación de la norma especial, que contempla de manera más específica el comportamiento ilícito. Por lo expuesto, solicita que, en la resolución definitiva, se desestime la aplicación del artículo 5.1.f) del RGPD al procedimiento que nos ocupa, y que los hechos se califiquen exclusivamente como una infracción del artículo 32 del mismo Reglamento, de acuerdo con el principio de especialidad.

Expone que la conducta antijurídica sancionada es única, y debe ser subsumida en el artículo 32 del RGPD, que es la norma que más exactamente se ajusta a los hechos y que aplicar tanto el artículo 5.1.f) como el artículo 32, no solo es contrario a la doctrina del TJUE y del Tribunal Supremo, sino que también resulta desproporcionado, tal y como ha subrayado el Comité Europeo de Protección de Datos en sus Directrices sobre el cálculo de sanciones.

Sin embargo, como afirma la Audiencia Nacional en su sentencia, de 8 de febrero de 2024 (recurso 2250/2021), el art. 32, aunque relacionado con el art. 5.1.f), no circunscribe el principio en su totalidad que requiere para su aplicación una pérdida de confidencialidad. Pérdida de confidencialidad de los datos acompañada de medidas de seguridad insuficientes

Además, las medidas cuya aplicación garantizaría la confidencialidad de los datos, como resulta obvio, no pueden limitarse, como afirma XFERA, exclusivamente a medidas de seguridad, debiendo ser contempladas con otras garantías que vayan más allá de las exclusivas medidas de seguridad.

En este sentido el párrafo 83 de las Directrices 4/2019 señala que *"(…) La seguridad de los datos personales requiere medidas adecuadas concebidas para prevenir y gestionar incidentes de vulneración de datos, para garantizar la debida ejecución de las tareas de tratamiento de datos y el cumplimiento de otros principios, y para facilitar el ejercicio efectivo de los derechos de las personas*".

Pues bien, tomando en consideración lo expuesto se concluye que en el supuesto analizado sí existió una pérdida de confidencialidad debido a la aplicación de medidas deficientes, por lo que ha de entenderse vulnerado el artículo 5.1.f) del RGPD y, ello, sin perjuicio de que en este caso se haya conculcado también el art. 32 del RGPD.

Por otro lado, debe tenerse en cuenta que el apartado 30 de las Directrices 04/22 sobre el cálculo de las multas administrativas contempladas en el RGPD, establece que:

"*El principio de concurso de infracciones (también denominado «concurso aparente» o «falso concurso») se aplica siempre que la aplicación de una disposición impida o abarque la aplicabilidad de la otra. En otras palabras, el concurso ya se produce en el nivel abstracto de las disposiciones legales. Esto podría basarse en los principios de especialidad, subsidiariedad o consunción, que se suelen aplicar cuando las disposiciones protegen el mismo interés jurídico. En tales casos, sería ilegal sancionar dos veces al infractor por la misma infracción."*

En relación con esta cuestión, esta Agencia considera necesario señalar que no cabe aplicar el principio de especialidad, subsidiariedad ni del consumo (no existe concurso medial de infracciones) porque los intereses jurídicos protegidos por los artículos imputados son diferentes. Mientras que el artículo 5.1.f) del RGPD tiene por finalidad el garantizar la confidencialidad y la integridad de los datos personales, el artículo 32 del RGPD tiene por finalidad adoptar y aplicar medidas para garantizar un nivel de seguridad adecuado al riesgo. Por tanto, en el primer caso, el interés jurídico protegido es la confidencialidad e integridad de los datos personales, mientras que en el segundo lo es la seguridad del tratamiento.

La independencia de ambos preceptos y, por tanto, el hecho de que sea posible cometer dos infracciones independientes, se deduce de la propia configuración que el legislador comunitario ha realizado de ambos tipos infractores: tipificándolos en dos preceptos diferentes: artículo 5.1.f) y artículo 32 del RGPD.

En cuanto a las condiciones generales para la imposición de multas administrativas que establece el RGPD, la vulneración del art. 5.1.f) del RGPD se encuentra tipificada en el artículo 83.5.a), mientas que la vulneración del artículo 32 del RGPD se tipifica en el artículo 83.4.a), siendo también distinto el límite máximo de las multas previstas (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, para el artículo 5.1.f) o 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, para el artículo 32 del RGPD).

Por otro lado, la LOPDGDD realiza una la calificación de las infracciones a efectos de prescripción diferente: mientras que la vulneración del art. 5.1.f) del RGPD es calificada a los efectos de la prescripción en el artículo 72.1.a) de la LOPDGDD; la vulneración del artículo 32 del RGPD es calificada a los efectos de la prescripción en el artículo 73.f) de la LOPDGDD y de igual forma, la infracción del art. 5.1.f) del RGPD prescribe a los tres años (siendo calificada como muy grave a los efectos de la

prescripción), mientras que la infracción del art. 32 del RGPD prescribe a los dos años (siendo calificada como grave a los efectos de la prescripción).

Incluso la forma de cumplir con cada obligación está configurada de forma diferente: 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.

Tal y como señala el apartado 34 de las Directrices 04/22 del CEPD: "*34. En cambio, cuando dos disposiciones persiguen objetivos autónomos, esto constituye un factor diferenciador que justifica la imposición de multas distintas. Por ejemplo, si la infracción de una disposición da lugar automáticamente a la infracción de la otra, pero no es así si la situación es la inversa, estas infracciones persiguen objetivos autónomos."*

No cabe duda de que ambas normas persiguen objetivos distintos. Mientras que el artículo 5.1.f) del RGPD tiene por objetivo el garantizar la confidencialidad y la integridad de los datos personales, el artículo 32 del RGPD tiene por objetivo adoptar y aplicar medidas para garantizar un nivel de seguridad adecuado al riesgo.

En definitiva, concurren una pluralidad de acciones, en la medida en que se han cometido dos conductas infractoras diferentes que han dado lugar a la vulneración de intereses jurídicos protegidos diferentes en cuyo caso, no cabe duda de que deben imputarse y sancionarse dos infracciones administrativas independientes.

Por las razones expuestas, no se entiende vulnerado el principio de especialidad.

CUARTA. La actuación de Xfera fue diligente; adecuación y correcta implementación de las medidas de seguridad.

Entrando en el fondo del asunto, alega que el presente expediente trae causa de un incidente de seguridad que fue identificado por los procesos internos de monitorización de la empresa, que detectaron un comportamiento anómalo a través de una aplicación utilizada en sus servicios de interacción con clientes (puntos de venta, call centers, atención al cliente, etc.). Estas consultas, afirma, que fueron realizadas con credenciales válidas de un usuario autorizado, quien manifestó no haber realizado dicha actividad. Manifiesta que, de manera inmediata, Xfera desactivó la cuenta y trató el incidente como un posible ataque de exfiltración de datos.

Expone que Xfera respondió con celeridad al detectar la brecha, activando las medidas necesarias para restaurar la seguridad del sistema y notificando tanto a la AEPD como a los clientes afectados y complementando esta información con posterioridad. Alega que, durante todo el proceso, la empresa siguió los protocolos establecidos a tal efecto, implementando mejoras significativas en sus políticas de seguridad para evitar que incidentes similares se repitan en el futuro. Le sorprende que esta autoridad considere las medidas reactivas adoptadas tras la brecha como una prueba de insuficiencia preventiva: todo lo contrario, en su opinión son una muestra del compromiso de Xfera con la protección de los datos personales y la mejora continua de sus sistemas.

4.1. Las medidas implementadas por Xfera eran adecuadas.

(…). Por dicha razón, este es un proceso donde la diligencia prestada por la entidad investigada es fundamental para evitar este tipo de vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que el tratamiento de datos sea conforme al RGPD.

Resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), partiendo de que se trata de entidades cuya actividad lleva aparejado un continuo tratamiento de datos de clientes, la cual indica que "…*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 prevenciones legales al respecto*".

(…).

Es decir, un tercero no autorizado consiguió acceder a los datos personales de sus clientes, sin que las medidas de seguridad que afirma XFERA que existían, lo impidieran ni lo detectaran de forma temprana, lo que constituye la infracción del art. 5.1.f) del RGPD.

Así pues, estamos ante conductas típicas, antijuridicas y culpables.

4.2. No es razonable interpretar las medidas reactivas como insuficiencia preventiva.

Procede reseñar que las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, no pueden ser en modo alguno sólo medidas reactivas, es decir, exclusivamente para solucionar de forma inmediata una brecha de datos personales después de sucedida. La mejora de los sistemas de monitorización y la revisión de las políticas de autenticación, si bien constituyeron un avance significativo en la protección de la seguridad de los datos, este avance llegó tardíamente, en un momento reactivo, lo que no quiere decir que esta AEPD las tenga en cuenta para evidenciar la ausencia de medidas previas

La ausencia de medidas para mitigar el riesgo, derivado de la realización de trabajos en los DNS que permitieron la desactivación del proxy de autenticación en la aplicación VFR, denota una deficiente identificación, análisis y valoración del riesgo. Es decir, una inadecuada evaluación de este riesgo. Además, XFERA tampoco detectó la falta de funcionamiento del 2FA durante todo el tiempo que este mecanismo estuvo desactivado.

4.3. La retirada del IBAN de la aplicación VFR se realizó para evitar futuros fraudes.

Se rechazan las alegaciones aducidas en este sentido, tras constatarse que un tercero accedió a los datos personales de sus clientes, sin garantizar la seguridad adecuada de estos, debiendo significarse que el cumplimiento de la obligación impuesta al

responsable no puede ser apreciado para atenuar la responsabilidad que se imputa XFERA por cuanto es una actuación debida y obligada por la Ley.

El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los "*riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (artículo 24.1)* y aplicando las medidas oportunas.

En este caso el IBAN se encontraba sin cifrar ni anonimizar lo que hubiera evitado que el atacante tuviera acceso a ese dato, sin que XFERA haya justificado la necesidad de que el empleado tuviera acceso a la totalidad de los dígitos que integran el código IBAN.

4.4. Del cierre de actuaciones por la División de Innovación Tecnológica de la AEPD.

En cuanto a este apartado, nos remitimos a lo dispuesto en el apartado segundo de este Fundamento de Derecho.

Asimismo, precede reseñar que la AEPD, tras la realización de las investigaciones oportunas, y en relación con una serie de hechos concretos que considera probados, incardina los mismos en el tipo infractor que considera adecuado, conforme a la aplicación e interpretación de la normativa, motivando de manera prolija y suficiente tal actuación. Y es que la AEPD se encuentra vinculada por el principio de legalidad que implica la aplicación e interpretación de las normas atendiendo al supuesto de hecho específico que concurra en cada caso.

4.5. Xfera como víctima de una actuación criminal respecto a la que se ha decretado secreto de sumario.

En cuanto a la condición de XFERA de haber sido víctima de una actuación criminal, 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.

4.6. Conclusión: vulneración del principio de culpabilidad.

Se recuerda que el principio de responsabilidad previsto en el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."*

No obstante, según lo dictaminado en la STS 7887/2011 de 24 de noviembre de 2011, Rec. 258/2009, "(…) desde su sentencia 76/1990, de 26 de abril, el Tribunal Constitucional viene declarando que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, doctrina que se reafirma en la sentencia 164/2005, de 20 de junio de 2005 , en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad aun a título de mera negligencia. Ahora bien, el modo de atribución de responsabilidad, a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana.

Sucede así que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad (véase la sentencia de esta Sala del Tribunal Supremo de 20 de noviembre de 2011 (recurso de casación en interés de ley 48/2007), éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas. Según la STC 246/1991 "(...) *esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma*."

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en la STS 6262/2009, de 9 de octubre de 2009, Rec 5285/2005, y STS 6336/2009, de 23 de octubre de 2009, Rec 1067/2006, que "*aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa*".

En el caso que se examina, se considera que XFERA ha actuado con negligencia. Como depositaria de datos de carácter personal a gran escala, por lo tanto, habituada o dedicada específicamente a la gestión de los datos de carácter personal de los clientes, debe ser especialmente diligente y cuidadosa en su tratamiento. Es decir, desde la óptica de la culpabilidad, estamos ante un error vencible, ya que, con las medidas técnicas y organizativas adecuadas, estos accesos indebidos se hubieran podido evitar. A mayor abundamiento, no podemos hablar tan sólo de una cuestión puntual y técnica prácticamente imprevisible, desde el momento en que ha sido necesario implementar medidas como la mejora de los sistemas de monitorización y la revisión de las políticas de autenticación.

En ningún caso se ha exigido una infalibilidad total de las medidas que se pueden adoptar para garantizar una protección adecuada en el tratamiento de los datos personales. El hecho de que se haya apreciado que el responsable de tratamiento contara con algunas medidas de seguridad, no obsta a que la brecha afectara a un volumen aproximado de ***CANTIDAD.4 de la entidad, filtrándose la siguiente tipología de datos personales: nombre y apellidos, fecha de nacimiento, número de NIF, correo

electrónico, números de teléfono, IBAN de la cuenta asociada y dirección física. Los datos no estaban cifrados, anonimizados o protegidos de forma ininteligible. La propia entidad afirma que *"pudieron comprobar que habían accedido a la API que consulta contra la base de datos y habían extraído información perteneciente a aproximadamente un millón setecientos mil clientes actuales de la operadora YOIGO."*

(…), constituye una manifestación de la debilidad de las medidas existentes en el momento de los hechos, lo que constituye una vulneración del principio de confidencialidad, establecido en el citado artículo 5.1.f) del RGPD.

En este sentido, no debe olvidarse, tal y como ha quedado expuesto en las actuaciones de investigación y de la información transmitida, que los atacantes accedieron y exfiltraron datos personales de los clientes.

Este nivel de acceso aumenta el riesgo de uso indebido y fraude y pone de manifiesto que las medidas técnicas y organizativas adoptadas por el responsable no eran las apropiadas para garantizar la integridad y confidencialidad adecuada de los datos personales, en especial para la protección contra el tratamiento no autorizado o ilícito.

Por otro lado, trae a colación lo 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).

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* [...]".

Por tanto, de la Sentencia se infiere que las obligaciones que se imponen al responsable de implantar medidas adecuadas constituyen una obligación de medios, pero 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, lo que ocurre en este caso, pues si bien existía el mecanismo 2FA en la aplicación VFR, este quedó sin efecto, permitiéndose el acceso al aplicativo sin necesidad de introducir clave OTP (solo con usuario y contraseña), sin que existieran medidas previas para evitar la pérdida de eficacia de la medida ni para detectar el fallo, toda vez que fue el 20 de febrero, cuando a raíz de un trabajo programado sobre el DNS, se deshabilitó el acceso a VFR a través del proxy de autenticación, y el fallo no se conoce hasta el 28 o 29 de marzo de 2023.

En consideración a lo expuesto no puede prosperar la cuestión planteada por la entidad investigada, debiendo ser rechazada.

QUINTA. Falta de proporcionalidad de la sanción.

En primer lugar, cabe recordar que las medidas correctivas de las que se dota a las Autoridades de Control se configuran en el RGPD como “poderes” esto es, como potestades de actuación que, lógicamente, se aplicarán en atención a las circunstancias presentes en cada caso concreto.

Por otro lado, esta Agencia desea señalar lo que el Considerando 148 del RGPD indica sobre la posibilidad de imponer un apercibimiento:

“En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante.”

En atención a los términos en los que se pronuncia, el RGPD insta con carácter general a la imposición de multas y prevé que el apercibimiento sea la medida utilizada cuando la infracción sea leve- circunstancia que no sucede en este caso- o implique una carga desproporcionada cuando la infracción haya sido cometida por una persona física.

En este sentido, esta Agencia ha evaluado y motivado todas las circunstancias agravantes o atenuantes a que hace referencia el citado considerando 148 del RPGD (que no son otras que las del artículo 83.2 del RGPD) y toda vez que las infracciones en cuestión no son leves a efectos del RGPD, se considera conforme a Derecho imponer una multa en vez de dirigir un apercibimiento. Razón por la que se desestima la presente alegación.

En cuanto al principio de proporcionalidad, la STS, Sala 3ª, de 16 de diciembre de 2003 (Rec. 4996/98) ya señalaba que el principio de proporcionalidad de las sanciones exige que "*la discrecionalidad que se otorga a la Administración para la aplicación de la sanción se desarrolle ponderando en todo caso las circunstancias concurrentes, al objeto de alcanzar la debida proporcionalidad entre los hechos imputados y la responsabilidad exigida".* Principio de proporcionalidad que no se entiende vulnerado, considerándose proporcionada la sanción propuesta a la entidad, por los hechos probados y ponderadas las circunstancias concurrentes, que se detallan más adelante. En el presente caso, se han cometido dos conductas infractoras diferentes que han dado lugar a la vulneración de intereses jurídicos protegidos diferentes en cuyo caso, no cabe duda de que deben imputarse y sancionarse dos infracciones administrativas independientes

Esta Agencia desea señalar que el RGPD no obliga a que deban existir graves daños y/o perjuicios de la parte reclamante para constatar la existencia de infracción.

La naturaleza de la infracción, número de afectados, la existencia o no de daños y perjuicios, son todas cuestiones que se han tenido en cuenta y han sido debidamente motivadas a la hora de graduar la sanción a imponer a XFERA.

Ahora bien, frente a lo alegado, procede señalar varias cosas:

En primer lugar, el artículo 83.1 RGPD establece que las multas administrativas por las infracciones del RGPD deben ser "…*en cada caso individual efectivas, proporcionadas y disuasorias*", indicando a continuación en el apartado 2 del citado precepto, que "*Las multas administrativas se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas*…" (el subrayado es nuestro). Estableciendo a continuación determinadas circunstancias a tener en cuenta.

Así, el cálculo del importe de las multas queda a decisión de la autoridad de control, con sujeción a las normas previstas en el RGPD.

En este contexto, el RGPD exige, como se ha señalado, que el importe de la multa sea en cada caso efectivo, proporcionado y disuasorio (artículo 83, apartado 1, del RGPD). Además, al fijar el importe de la multa, las autoridades de control tendrán debidamente en cuenta una lista de circunstancias que se refieren a las características de la infracción (su gravedad) o al carácter del autor (artículo 83, apartado 2, del RGPD).

Por último, el importe de la multa no excederá de los importes máximos previstos en el artículo 83, apartado 4, apartados 5 y 6, del RGPD.

Por lo tanto, la cuantificación del importe de la multa se basa en una evaluación específica realizada en cada caso, dentro de los parámetros previstos por el RGPD. Además, debe tenerse en cuenta que el cálculo de una multa no es un mero ejercicio matemático, siendo las circunstancias del caso específico los factores determinantes que conducen a la cantidad final, que puede ser, en todos los casos y para cada infracción, una cantidad distinta hasta el máximo legal.

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.

Por tanto, 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)

Recordemos en este punto lo manifestado por el TJUE en la sentencia dictada en el asunto C-683-21.

> *78 La existencia de un sistema de sanciones que permita imponer, cuando las circunstancias específicas de cada caso lo justifiquen, una multa administrativa con arreglo al artículo 83 del RGPD crea un incentivo para que los responsables y encargados del tratamiento cumplan el Reglamento. Con su efecto disuasorio, las multas administrativas contribuyen a reforzar la protección de las personas físicas en lo que respecta al tratamiento de datos personales y constituyen, por ende, un elemento clave para garantizar el respeto de los derechos de dichas personas, de conformidad con la finalidad del citado Reglamento de asegurar un elevado nivel de protección de esas personas en lo que respecta al tratamiento de los datos personales.*
>
> Asimismo, la reciente STJUE de 13 de febrero de 2025, en el asunto C-383/23, dispone que la imposición de una multa exige en el examen de cada caso particular de una serie de elementos previstos en el artículo 83 del RGPD, del que el volumen de negocios es un elemento más (ni el único ni el determinante), para imponer una multa que sea proporcional, disuasoria y efectiva y se refuerce, de esta forma, la protección de las personas físicas.
>
> *25 Así, en virtud del artículo 83, apartado 1, del RGPD, cada autoridad de control tiene que garantizar que las multas administrativas con arreglo al referido artículo 83 por las* infracciones *del RGPD indicadas en sus apartados 4 a 6 sean, en cada caso individual, efectivas, proporcionadas y disuasorias.*
> *26 Más allá del cumplimiento de estos tres requisitos, el apartado 2 de dicho artículo 83 exige, para decidir la imposición de una multa administrativa y su importe, que la autoridad de control competente tenga debidamente en cuenta, en cada caso individual, una serie de elementos.*

27 De conformidad con esta última disposición, entre esos elementos figuran, en particular, la naturaleza, gravedad y duración de la infracción, el número de interesados afectados y el nivel de los daños y perjuicios sufridos, la intencionalidad o negligencia en la infracción, las medidas adoptadas por el responsable o el encargado del tratamiento para paliar los daños y perjuicios sufridos, el grado de responsabilidad del responsable o del encargado del tratamiento y las categorías de datos personales afectados por la infracción.

28 Los citados elementos se refieren, bien al comportamiento de ese responsable o encargado, acusado de infringir determinadas disposiciones del RGPD, bien a las propias infracciones. Así pues, sirven para garantizar que cada una de dichas infracciones se aprecie sobre la base de todas las circunstancias individuales pertinentes y que se alcancen los objetivos perseguidos por el régimen sancionador contemplado en el RGPD.

29 Aunque estos elementos no hacen referencia al concepto de empresa, en el sentido de los artículos 101 TFUE y 102 TFUE, el Tribunal de Justicia ya ha declarado que solamente una multa que tenga en cuenta no solo todos los elementos que caractericen las infracciones del RGPD constatadas, sino también, en su caso, la capacidad económica real o material de su destinatario, reúne los tres requisitos establecidos en el artículo 83, apartado 1, del RGPD, a saber, ser a la vez efectiva, proporcionada y disuasoria. Pues bien, para apreciar estos requisitos, debe tenerse en cuenta si ese destinatario forma parte de una empresa en el sentido de los artículos 101 TFUE y 102 TFUE (véase, en este sentido, la sentencia de 5 de diciembre de 2023, Deutsche Wohnen, C 807/21, EU:C:2023:950, apartado 58).

En consecuencia, las alegaciones deben ser desestimadas.

SEXTA. Circunstancias aplicables al caso individual, conforme al art. 83.2 RGPD.

6.1. Naturaleza, gravedad y duración de la infracción.

A este respecto, procede señalar que estas circunstancias se tienen en cuenta para establecer el nivel de gravedad de las infracciones que se consideran cometidas. Pues bien, en este caso, se tiene en cuenta el elevado número de clientes de XFERA sobre los que se realizan operaciones de tratamiento referidas al tratamiento sobre el que se ha producido la brecha de datos personales: (…).*”*

En el caso que nos ocupa, el tipo de datos que trata y que fueron afectados por la brecha y que XFERA parece desdeñar, supone un riesgo alto, en caso de vulnerarse su confidencialidad, de ser usados de modo fraudulento: suplantación de la identidad phishing, fraude financiero, etc.

Lo que se trata de poner en evidencia es que la vulneración de las infracciones se halla acrecentada y agravada por el número de afectados por el incidente, los daños y perjuicios provocados (pérdida irreversible de poder y control de los datos personales por los clientes).

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*".

6.2. De la ausencia de perjuicio para los interesados afectados por la brecha.

En cuanto al argumento de que no consta la existencia de perjuicio material o económico como resultado de la brecha de seguridad de XFERA, en primer lugar, esta Agencia desea reiterar que el RGPD no obliga a que deban existir graves daños y/o perjuicios de la parte reclamante para constatar la existencia de infracción, como en el presente caso.

Y en segundo lugar no es causa de justificación o exculpación suficiente, toda vez que los afectados se han visto desprovistos del control sobre sus datos personales, algunos han sido víctimas de phishing y en algunos casos, con cargos desconocidos en la factura del teléfono. En este caso la búsqueda en internet, por ejemplo, del nombre, apellidos de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, permita el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular. Esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

6.3. Intencionalidad o negligencia en la sanción.

El hecho de que XFERA sea una empresa para cuya actividad realiza un constante y abundante manejo de datos personales, realizando tratamientos que implican un probable alto riesgo para los derechos y libertades de las personas físicas supone la exigencia de una diligencia mayor en la implantación de medidas para la protección de los datos personales que la que se pueda exigir a una pequeña empresa con menos recursos económicos y técnicos que XFERA y que realice un menor número de tratamientos, incluso esporádicos o accesorios.

Teniendo en cuenta que en la conducta de la entidad investigada concurre el elemento de culpabilidad, que es indispensable para poder exigir responsabilidad sancionadora, en este caso se concreta, además, en una muy grave falta de diligencia en la adopción de medidas adecuadas para la protección de los datos de carácter personal y para comprobar su cumplimiento como se ha puesto de manifiesto a lo largo del procedimiento.

Además, la falta de diligencia demostrada en la conducta infractora de la que se le responsabiliza debe calificarse de muy grave, pues datos de alta sensibilidad como el IBAN se encontraban en claro y sin cifrar. La entidad investigada está obligada en virtud del artículo 5.2 del RGPD a desplegar la actividad adecuada para cumplir los principios de protección de datos, por lo que aquí interesa, el de confidencialidad, y a estar en condiciones de demostrar su cumplimiento.

6.4. Medidas adoptadas para paliar los daños y perjuicios sufridos por los interesados.

Como se ha indicado anteriormente, la entidad no habría adoptado medidas para impedir que terceros no autorizados explotaran la vulnerabilidad identificada.

6.5. Infracciones anteriores cometidas por Xfera.

El considerando 148 del RGPD señala que:

"A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías."

Así pues, conforme al apartado e) del artículo 83.2. RGPD, en la determinación del importe de la sanción de multa administrativa no podrán dejar de valorarse todas aquellas infracciones anteriores del responsable o del encargado de tratamiento en aras a calibrar la antijuricidad de la conducta analizada o la culpabilidad del sujeto infractor.

Por tanto, las infracciones anteriores a la infracción objeto de examen más lejanas en el tiempo o menos próximas a la infracción actual sí deben ser tenidas en cuenta al decidir sobre la cuantía de la sanción, aunque como aclaran las Directrices sobre multas las autoridades podrán concederles menor transcendencia en la fijación del importe de la multa.

Además, una correcta interpretación de la disposición del artículo 83.2.e) RGPD no puede obviar la finalidad perseguida por la norma: decidir la cuantía de la sanción de multa administrativa en el caso individual planteado atendiendo siempre a que la sanción sea proporcional, efectiva y disuasoria.

En este caso, se han valorado adecuadamente y tenido en cuenta todas las circunstancias pertinentes, estableciéndose los importes de las multas en base a estas circunstancias, manteniendo al mismo tiempo, como se ha indicado, el carácter efectivo, disuasorio y proporcionado de la multa, que no supera el máximo legal aplicable.

Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que XFERA ha sido sancionada por la infracción de los artículos 5.1f) o 32 del RGPD. (Ej.: PS/00027/2021, PS/00448/2020, PS/00104/2020)

En el desarrollo de la actividad que le es propia, necesita de manera habitual tratar datos de carácter personal, lo que incide en la diligencia que le es exigible para el cumplimiento de los principios que presiden el tratamiento de datos de carácter personal y la calidad y efectividad de las medidas técnicas y organizativas que debe tener implementadas para garantizar el respeto de este derecho.

6.6. Adhesión a códigos de conducta o a mecanismos de certificación aprobados.

Finalmente, en cuanto a la adhesión a códigos de conducta o a mecanismos de certificación aprobados de cara a reforzar el cumplimiento en materia de protección de datos, se ha de indicar que XEFERA aporta como Documento n.º 15 certificado del Sistema de Gestión de seguridad de la Información conforme con la ISO 27001 para los sistemas de información que soportan los servicios de comunicaciones móviles y de conectividad fija.

También aporta, como Documento n.º 16, certificado el Sistema de Gestión de seguridad de la Información conforme con la norma Privacidad de la información ISO 27701, igualmente referida al sistema de gestión de privacidad que da soporte a los servicios de comunicaciones móviles y servicios de conectividad fija.

Por tanto, ninguna de las dos certificaciones afectaría a la seguridad de la Aplicación VFR.

En definitiva, aunque la documentación aportada por XFERA puede reflejar una conducta positiva, no desvirtúa los hechos constatados.

SÉPTIMA. Proposición de prueba.

A este respecto, resaltar que no ha aportado el informe pericial detallado en la carta de aceptación de encargo que se anexaba como Documento nº 18, relativo al análisis de las medidas de seguridad que pudiesen ser de interés en relación con este procedimiento. Así las cosas, se informa de que, de acuerdo con lo dispuesto en el artículo 89.2 de la LPACAP, notificada la Propuesta de resolución, podrá alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de las infracciones que se declaran cometidas ni suponen causa de justificación o exculpación suficiente.

IV
Alegaciones a la Propuesta de Resolución

En relación con las alegaciones aducidas a la Propuesta de Resolución, reiterándose básicamente en las alegaciones ya presentadas ante el Acuerdo de Inicio, debe señalarse que todas ellas ya fueron analizadas y desestimadas en el Fundamento de

Derecho III de la Propuesta de resolución, a la que, en aras de economía procesal, procede remitirse.

En cuanto al resto de alegaciones, se procede a dar respuesta a las mismas, según el orden expuesto:

PRIMERA. De la necesaria suspensión del procedimiento por prejudicialidad penal.

XFERA alega que los hechos objeto de este procedimiento sancionador se encuentran bajo investigación penal, como consecuencia de la denuncia presentada; investigación que ha recaído en el Juzgado de Instrucción n.º 28 de Madrid y está siendo sustanciada a través de las ******DILIGENCIAS.1***, en las que Xfera se ha personado como acusación particular.

En este caso, considera que nos encontramos ante una situación en la que los mismos hechos están siendo investigados en sede penal, y donde cualquier decisión administrativa prematura podría resultar contradictoria con lo que se resuelva en tal jurisdicción. Por ello, entiende que, en aplicación del principio de prejudicialidad penal, no debe resolverse el asunto en vía administrativa en tanto en cuanto no se resuelva por la vía penal dado que en este procedimiento concurren la triple identidad de sujeto, hecho y fundamento que exige la jurisprudencia para suspender la tramitación de un procedimiento sancionador por prejudicialidad penal.

A este respecto, debe tenerse en cuenta que el artículo 77.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas dispone que:

"*En los procedimientos de carácter sancionador, los hechos declarados probados por resoluciones judiciales penales firmes vincularán a las Administraciones Públicas respecto de los procedimientos sancionadores que substancien*".

En relación con esta cuestión, esta Agencia considera necesario señalar que, en el presente expediente sancionador no existe la triple identidad necesaria para aplicar el artículo 77.4 de la Ley 39/2015, de sujeto, hecho y fundamento entre la infracción administrativa que se valora y la posible o posibles infracciones penales que se pudieran derivar de la denuncia presentada ante el órgano jurisdiccional, en la medida en que el sujeto infractor no es el mismo.

De este modo, XFERA, con NIF A82528548, es el sujeto responsable en el presente procedimiento sancionador, mientras que el responsable penal de un presunto delito de estafa sería un tercero. Aspecto que XFERA no ignora pues ha esgrimido con insistencia en sus alegaciones al acuerdo de inicio, como un argumento a su favor, su condición de "*víctima de una actuación criminal".*

Tampoco el fundamento jurídico sería el mismo: mientras el bien jurídico protegido por el RGPD, es el derecho fundamental a la protección de datos personales, el bien jurídico que se protege en el tipo penal de estafa, cuya comisión investiga el Juzgado de Instrucción n.º 28 de Madrid, es el patrimonio ajeno.

En este sentido es muy esclarecedora la Sentencia de la Audiencia Nacional de 27/04/2012 (rec. 78/2010), en cuyo Fundamento Jurídico segundo el Tribunal se pronuncia en los siguiente términos frente al alegato de la recurrente de que la AEPD ha infringido el artículo 7 del R.D. 1398/1993 (norma que estuvo vigente hasta la entrada en vigor de la LPACAP): "*En este sentido el Art. 7 del Real Decreto 1398/1993, de 4 de agosto, del procedimiento para el ejercicio de la potestad sancionadora, únicamente prevé la suspensión del procedimiento administrativo cuando se verifique la existencia efectiva y real de un procedimiento penal, si se estima que concurre identidad de sujeto, hecho y fundamento de derecho entre la infracción administrativa y la infracción penal que pudiera corresponder.*

No obstante, y para la concurrencia de una prejudicialidad penal, se requiere que ésta condicione directamente la decisión que haya de tomarse o que sea imprescindible para resolver, presupuestos que no concurren en el caso examinado, en el que existe una separación entre los hechos por los que se sanciona en la resolución ahora recurrida y los que la recurrente invoca como posibles ilícitos penales. Así, y aun de haberse iniciado, en el presente supuesto, y por los hechos ahora controvertidos, también actuaciones penales frente a la empresa distribuidora, lo cierto es que tanto la conducta sancionadora como el bien jurídico protegido son distintos en una y otra vía (contencioso-administrativa y penal). En el ámbito penal, el bien jurídico protegido es una posible falsedad documental y estafa, y en el ámbito administrativo, en cambio, la facultad de disposición de sus datos personales por parte de su titular, por lo que tal objeción de la demandada ha de ser rechazada".

Por tanto, la cuestión planteada por Xfera no puede prosperar y debe ser rechazada.

SEGUNDA. – DE LA INSTRUCCIÓN DEL EXPEDIENTE AMINISTRATIVO POR LA AGENCIA.

Del examen de los hechos relativos al incidente de seguridad, afirma que la Agencia identifica como constitutivo de infracción, el mero hecho de que se produzca una brecha de seguridad y que se hayan presentado reclamaciones por quienes fueron diligentemente informados de la misma, siendo éste último hecho el único que, en su opinión, hace que la AEPD vuelva a reactivar un procedimiento, respecto al que ella misma había dictado que "*no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales"*, sin que se atienda, ni analice el concreto supuesto de hecho, la ausencia de perjuicio asociado o de publicación en abierto de los datos, las medidas de seguridad implementadas, ni las responsabilidades derivadas.

A este respecto, debe tenerse en cuanta que, en el encabezado del escrito de 12 de mayo de 2023, citado por XFERA, consta *"DIVISIÓN DE INNOVACIÓN TECNOLÓGICA*" y finaliza indicando que "*no están previstas más acciones por parte de esta División con relación a este acto de comunicación de brecha de datos personales*."

Por tanto, en contra de lo que afirma la entidad investigada, este escrito no tiene carácter decisorio, ni por su contenido (más bien es un "acuse de recibo" de la brecha notificada) que se encuentra circunscrito al acto de la notificación y a las posibles acciones de la División, y que en modo alguno puede entenderse como si esta AEPD

hubiese valorado que no concurría 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 la entidad, ni tampoco por su forma, pues ni siquiera formalmente refleja una decisión en tal sentido, ni mucho menos una resolución de archivo de actuación alguna, pues para que ello sea así, sería necesario que tales actuaciones se hubiesen iniciado.

Dicho escrito está encaminado a poner en conocimiento de XFERA la recepción de la notificación de la brecha acaecida y de su incorporación al registro de notificaciones de brechas, de acuerdo con lo determinado en el artículo 31.d) del Estatuto de la Agencia, aprobado mediante Real Decreto 389/2021, de 1 de junio, sin que pueda deducirse a la vista del mismo, que la AEPD valoró y decidió que no concurría responsabilidad alguna por un supuesto incumplimiento de la normativa de protección de datos. Únicamente informa que por la DIT no se prevé realizar más actuaciones relacionadas con el acto de comunicación de la brecha, pero todo ello sin perjuicio de que puedan iniciarse otras actuaciones, como resulta obvio.

Así, el artículo 13 del Estatuto de la AEPD 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.

El artículo 57, Funciones, del RGPD en su letra h) establece que:

"1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

(…)

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particu-lar basándose en información recibida de otra autoridad de control u otra autoridad pú-blica;

(…)

En cuanto a las funciones de la Subdirección General de Inspección de Datos de la AEPD, el artículo 27 del Estatuto de la Agencia indica, en su apartado 1, que:

"La Subdirección General de Inspección de Datos es el órgano administrativo, depen-diente 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 ci-tado Reglamento"

Y en el apartado 2 de este artículo 27 enumera las funciones que corresponden a la Subdirección General de Inspección de Datos de Datos, entre las que se encuentran, por lo que aquí interesa, las siguientes:

"a) La supervisión permanente del cumplimiento del Reglamento (UE) 2016/679 del Par-lamento 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 presen-tada ante la Agencia Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 77.2 del citado Reglamento.

(…)"

Por tanto, para proceder al archivo de unas actuaciones investigación se requiere, primero, que se hayan iniciado, lo cual no había sucedido en el momento de emitirse el referido escrito de la División de Innovación Tecnológica y, en segundo lugar, es necesaria una resolución expresa por parte de la Presidencia de la Agencia Española de Protección de Datos, 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, se presentaron distintas reclamaciones de clientes a los que la operadora había comunicado el incidente.

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 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

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.

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.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

En relación con las actuaciones previas de investigación el art. 67 de la LOPDGDD dispone lo siguiente:

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 dieciocho 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.

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 la existencia o no 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 concurren los elementos necesarios para la apertura de un procedimiento sancionador. 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, y como indica el artículo 67.2 LOPDGDD referenciado, la AEPD puede llevar a cabo actuaciones previas de investigación. Lo que aconteció en este caso, a fin de lograr una mejor determinación de los hechos y las circunstancias. Es una potestad que tiene atribuida a la AEPD por el RGPD y por la LOPDGDD.

Asimismo, y a mayor abundamiento, incluso en el supuesto de no haber existido las reclamaciones, el escrito cuestionado 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 presentadas en esta AEPD, 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.

A este respecto, se recuerda de nuevo que dichas reclamaciones, sólo se admiten, siendo la documentación y todo lo recopilado durante dichas actuaciones de investigación, lo que ha motivado, exclusivamente, el inicio del presente procedimiento sancionador, y no las citadas reclamaciones.

TERCERO Y CUARTO. -SOBRE EL SUPUESTO INCUMPLIMIENTO DE LO DISPUESTO EN EL ARTÍCULO 5.1 f) y 32 DEL RGPD.

Se reitera que en el supuesto analizado sí existió una pérdida de confidencialidad debido a la aplicación de medidas deficientes, por lo que ha de entenderse vulnerado el artículo 5.1.f) del RGPD y, ello, sin perjuicio de que en este caso se haya conculcado también el art. 32 del RGPD.

Por otro lado, debe tenerse en cuenta que el apartado 30 de las Directrices 04/22 sobre el cálculo de las multas administrativas contempladas en el RGPD, establece que:

"*El principio de concurso de infracciones (también denominado «concurso aparente» o «falso concurso») se aplica siempre que la aplicación de una disposición impida o*

abarque la aplicabilidad de la otra. En otras palabras, el concurso ya se produce en el nivel abstracto de las disposiciones legales. Esto podría basarse en los principios de especialidad, subsidiariedad o consunción, que se suelen aplicar cuando las disposiciones protegen el mismo interés jurídico. En tales casos, sería ilegal sancionar dos veces al infractor por la misma infracción."

En relación con esta cuestión, esta Agencia considera necesario señalar que no cabe aplicar el principio de especialidad, subsidiariedad ni del consumo (no existe concurso medial de infracciones) porque los intereses jurídicos protegidos por los artículos imputados son diferentes. Mientras que el artículo 5.1.f) del RGPD tiene por finalidad el garantizar la confidencialidad y la integridad de los datos personales, el artículo 32 del RGPD tiene por finalidad adoptar y aplicar medidas para garantizar un nivel de seguridad adecuado al riesgo. Por tanto, en el primer caso, el interés jurídico protegido es la confidencialidad e integridad de los datos personales, mientras que en el segundo lo es la seguridad del tratamiento.

La independencia de ambos preceptos y, por tanto, el hecho de que sea posible cometer dos infracciones independientes, se deduce de la propia configuración que el legislador comunitario ha realizado de ambos tipos infractores: tipificándolos en dos preceptos diferentes: artículo 5.1.f) y artículo 32 del RGPD. Por un lado, se incumple el art. 5.1.f) cuando una deficiente implantación de medidas técnicas y organizativas conlleva la pérdida de confidencialidad o integridad, y, por otro lado, se incumple el art. 32 del RGPD cuando las medidas de seguridad aplicadas por el responsable no garantizan la seguridad de los datos, sin que en este caso se requiera la existencia de una pérdida de confidencialidad o integridad.

En cuanto a las condiciones generales para la imposición de multas administrativas que establece el RGPD, la vulneración del art. 5.1.f) del RGPD se encuentra tipificada en el artículo 83.5.a), mientas que la vulneración del artículo 32 del RGPD se tipifica en el artículo 83.4.a), siendo también distinto el límite máximo de las multas previstas (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, para el artículo 5.1.f) o 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, para el artículo 32 del RGPD).

Por otro lado, la LOPDGDD realiza una la calificación de las infracciones a efectos de prescripción diferente: mientras que la vulneración del art. 5.1.f) del RGPD es calificada a los efectos de la prescripción en el artículo 72.1.a) de la LOPDGDD; la vulneración del artículo 32 del RGPD es calificada a los efectos de la prescripción en el artículo 73.f) de la LOPDGDD y de igual forma, la infracción del art. 5.1.f) del RGPD prescribe a los tres años (siendo calificada como muy grave a los efectos de la prescripción), mientras que la infracción del art. 32 del RGPD prescribe a los dos años (siendo calificada como grave a los efectos de la prescripción).

Incluso la forma de cumplir con cada obligación está configurada de forma diferente: 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 por ausencia o

deficiencia de las medidas técnicas u organizativas que no tienen por qué ser de seguridad.

Tal y como señala el apartado 34 de las Directrices 04/22 del CEPD: "*34. En cambio, cuando dos disposiciones persiguen objetivos autónomos, esto constituye un factor diferenciador que justifica la imposición de multas distintas. Por ejemplo, si la infracción de una disposición da lugar automáticamente a la infracción de la otra, pero no es así si la situación es la inversa, estas infracciones persiguen objetivos autónomos."*

No cabe duda de que ambas normas persiguen objetivos distintos. Mientras que el artículo 5.1.f) del RGPD tiene por objetivo el garantizar la confidencialidad y la integridad de los datos personales, el artículo 32 del RGPD tiene por objetivo adoptar y aplicar medidas para garantizar un nivel de seguridad adecuado al riesgo.

En definitiva, concurren una pluralidad de acciones, en la medida en que se han cometido dos conductas infractoras diferentes que han dado lugar a la vulneración de intereses jurídicos protegidos diferentes en cuyo caso, no cabe duda de que deben imputarse y sancionarse dos infracciones administrativas independientes.

Por las razones expuestas, no se entiende vulnerado el principio de especialidad.

-La actuación de Xfera fue diligente; adecuación y correcta implementación de las medidas de seguridad.

Entrando en el fondo del asunto, alega que el presente expediente trae causa de un incidente de seguridad que fue identificado por los procesos internos de monitorización de la empresa, que detectaron un comportamiento anómalo a través de una aplicación utilizada en sus servicios de interacción con clientes (puntos de venta, call centers, atención al cliente, etc.). Estas consultas, afirma, que fueron realizadas con credenciales válidas de un usuario autorizado, quien manifestó no haber realizado dicha actividad. Manifiesta que, de manera inmediata, Xfera desactivó la cuenta y trató el incidente como un posible ataque de exfiltración de datos.

Expone que Xfera respondió con celeridad al detectar la brecha, activando las medidas necesarias para restaurar la seguridad del sistema y notificando tanto a la AEPD como a los clientes afectados y complementando esta información con posterioridad. Alega que, durante todo el proceso, la empresa siguió los protocolos establecidos a tal efecto, implementando mejoras significativas en sus políticas de seguridad para evitar que incidentes similares se repitan en el futuro. Le sorprende que esta autoridad considere las medidas reactivas adoptadas tras la brecha como una prueba de insuficiencia preventiva: todo lo contrario, en su opinión son una muestra del compromiso de Xfera con la protección de los datos personales y la mejora continua de sus sistemas.

-Las medidas implementadas por Xfera eran adecuadas.

(…). En este sentido, fue necesario que un tercero accediese a los datos de los clientes, haciendo un tratamiento de esos datos, ya que tuvo acceso a ellos. Por dicha razón, este es un proceso donde la diligencia prestada por la entidad investigada es

fundamental para evitar este tipo de vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que el tratamiento de datos sea conforme al RGPD.

Resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), partiendo de que se trata de entidades cuya actividad lleva aparejado un continuo tratamiento de datos de clientes, la cual indica que "…*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 prevenciones legales al respecto*".

(…).

Pero, es más, por otro lado, se ha producido el acceso y exfiltración por un tercero no autorizado de los datos de los clientes de Xfera, sin que las medidas aplicadas por XFERA alertaran del ataque de forma temprana, a pesar de que todos los accesos se realizaron utilizando las credenciales de un mismo usuario. Así, los resultados de la investigación apuntan a que la brecha afectó a un volumen aproximado de (…).

La propia entidad afirma que *"(…)."*

Es decir, un tercero no autorizado consiguió acceder a los datos personales de sus clientes, sin que las medidas de seguridad que afirma XFERA que existían, lo impidieran ni lo detectaran de forma temprana, lo que constituye la infracción del art. 5.1.f) del RGPD.

Así pues, estamos ante conductas típicas, antijuridicas y culpables.

-No es razonable interpretar las medidas reactivas como insuficiencia preventiva.

Procede reseñar que las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, no pueden ser en modo alguno sólo medidas reactivas, es decir, exclusivamente para solucionar de forma inmediata una brecha de datos personales después de sucedida. La mejora de los sistemas de monitorización y la revisión de las políticas de autenticación, si bien constituyeron un avance significativo en la protección de la seguridad de los datos, este avance llegó tardíamente, en un momento reactivo, lo que no quiere decir que esta AEPD las tenga en cuenta para evidenciar la ausencia de medidas previas, es decir de ningún modo esta AEPD interpreta que la aplicación de medidas reactivas se traduce en una insuficiencia de las medidas preventivas existentes.

(…).

-La retirada del IBAN de la aplicación VFR se realizó para evitar futuros fraudes.

Se rechazan las alegaciones aducidas en este sentido, tras constatarse que un tercero accedió a los datos personales de sus clientes, sin garantizar la seguridad adecuada de estos, debiendo significarse que el cumplimiento de la obligación impuesta al responsable no puede ser apreciado para atenuar la responsabilidad que se imputa XFERA por cuanto es una actuación debida y obligada por la Ley.

El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los "*riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (artículo 24.1)* y aplicando las medidas oportunas.

(…).

-Del cierre de actuaciones por la División de Innovación Tecnológica de la AEPD.

En cuanto a este apartado, nos remitimos a lo dispuesto en el apartado segundo de este Fundamento de Derecho.

Asimismo, precede reseñar que la AEPD, tras la realización de las investigaciones oportunas, y en relación con una serie de hechos concretos que considera probados, incardina los mismos en el tipo infractor que considera adecuado, conforme a la aplicación e interpretación de la normativa, motivando de manera prolija y suficiente tal actuación. Y es que la AEPD se encuentra vinculada por el principio de legalidad que implica la aplicación e interpretación de las normas atendiendo al supuesto de hecho específico que concurra en cada caso.

-Xfera como víctima de una actuación criminal respecto a la que se ha decretado secreto de sumario.

En cuanto a la condición de XFERA de haber sido víctima de una actuación criminal, 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.

QUINTA. - DE LA INADMISIÓN DE LA RESPONSABILIDAD OBJETIVA.

Se recuerda que el principio de responsabilidad previsto en el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."*

No obstante, según lo dictaminado en la STS 7887/2011 de 24 de noviembre de 2011, Rec. 258/2009, "(…) desde su sentencia 76/1990, de 26 de abril, el Tribunal Constitucional viene declarando que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, doctrina que se reafirma en la sentencia 164/2005, de 20 de junio de 2005 , en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad aun a título de mera negligencia. Ahora bien, el modo de atribución de responsabilidad, a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana.

Sucede así que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad (véase la sentencia de esta Sala del Tribunal Supremo de 20 de noviembre de 2011 (recurso de casación en interés de ley 48/2007), éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas. Según la STC 246/1991 "(...) *esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma*."

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en la STS 6262/2009, de 9 de octubre de 2009, Rec 5285/2005, y STS 6336/2009, de 23 de octubre de 2009, Rec 1067/2006, que "*aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa*".

En el caso que se examina, se considera que XFERA ha actuado con negligencia. Como depositaria de datos de carácter personal a gran escala, por lo tanto, habituada o dedicada específicamente a la gestión de los datos de carácter personal de los clientes, debe ser especialmente diligente y cuidadosa en su tratamiento. Es decir, desde la óptica de la culpabilidad, estamos ante un error vencible, ya que, con las medidas técnicas y organizativas adecuadas, estos accesos indebidos se hubieran podido evitar. A mayor abundamiento, no podemos hablar tan sólo de una cuestión puntual y técnica prácticamente imprevisible, desde el momento en que ha sido necesario implementar medidas como la mejora de los sistemas de monitorización y la revisión de las políticas de autenticación.

En ningún caso se ha exigido una infalibilidad total de las medidas que se pueden adoptar para garantizar una protección adecuada en el tratamiento de los datos personales. El hecho de que se haya apreciado que el responsable de tratamiento contara con algunas medidas de seguridad, no obsta a que la brecha afectara a un volumen aproximado de ***CANTIDAD.4 (…)*."*

(…), constituye una manifestación de la debilidad de las medidas existentes en el momento de los hechos, lo que constituye una vulneración del principio de confidencialidad, establecido en el citado artículo 5.1.f) del RGPD.

En este sentido, no debe olvidarse, tal y como ha quedado expuesto en las actuaciones de investigación y de la información transmitida, que los atacantes accedieron y exfiltraron datos personales de los clientes.

Este nivel de acceso aumenta el riesgo de uso indebido y fraude y pone de manifiesto que las medidas técnicas y organizativas adoptadas por el responsable no eran las apropiadas para garantizar la integridad y confidencialidad adecuada de los datos personales, en especial para la protección contra el tratamiento no autorizado o ilícito.

Por otro lado, trae a colación lo 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).

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 [...]".

Por tanto, de la Sentencia se infiere que las obligaciones que se imponen al responsable de implantar medidas adecuadas constituyen una obligación de medios, pero también deja claro que deben existir medidas adecuadas para evitar o mitigar el riesgo que no fueron aplicadas, ello supone un incumplimiento de la citada obligación impuesta por el RGPD y, por ende, una infracción al mismo, lo que ocurre en este caso, (…).

En consideración a lo expuesto no puede prosperar la cuestión planteada por la entidad investigada, debiendo ser rechazada.

SEXTA. SOBRE LA EXISTENCIA DE UN CONCURSO MEDIAL.

Alega que los hechos que se imputan a Xfera han sido calificados, en el Acuerdo de Inicio, como constitutivos de dos infracciones diferenciadas: por un lado, la vulneración del artículo 5.1.f) del RGPD, tipificada como infracción muy grave, y por otro, el incumplimiento del artículo 32 del RGPD, tipificada como grave.

Considera que el Acuerdo de Inicio explica que la primera sanciona la pérdida de confidencialidad de los datos personales, mientras que la segunda reacciona frente a la insuficiencia de las medidas de seguridad implementadas. Sin embargo, esta calificación resulta, en su opinión, incorrecta, ya que ambas infracciones se aplican sobre una misma conducta y persiguen proteger el mismo bien jurídico, lo que vulnera los dos principios expuestos.

Vulneración del principio non bis in ídem

Afirma que en el caso que nos ocupa, las dos infracciones propuestas por la Agencia buscan sancionar la misma conducta: la supuesta falta de adopción de medidas técnicas y organizativas suficientes para garantizar la seguridad de los datos personales. No existe, por tanto, en su opinión, una pluralidad de conductas que pueda justificar la doble sanción.

En primer lugar, indicar que los artículos 5.1 f) y 32 del RGPD se tipifican de manera diferenciada en el RGPD. Asimismo, se califican en la LOPDGDD de manera diferenciada, a los efectos de la prescripción, y gozan, cada uno de ellos, de entidad propia.

En el escrito de alegaciones al acuerdo de inicio, XFERA afirma: "*que la conducta sancionada, que es la falta de adopción de medidas de seguridad adecuadas, ha provocado la pérdida de confidencialidad: sin una, no se habría producido la otra. (…) Ambas infracciones, por tanto, derivan de la misma conducta y se relacionan con el mismo bien jurídico, lo que refuerza la idea de que la doble sanción vulnera el principio non bis in ídem.*"

Esta falta de diferenciación entre los hechos sancionados en cada infracción es precisamente lo que le lleva a concluir que se ha vulnerado el principio non bis in ídem.

Pues bien, en relación con las alegaciones que acaban de ser reproducidas, resulta necesario traer a colación la diferencia entre la vulneración del art. 5.1.f) y la del artículo 32 de RGPD, la diferente tipificación en apartados 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 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 e integridad cuando explicita "*mediante la aplicación de medidas técnicas y organizativas apropiadas*", que no son estrictamente de seguridad.

Existen 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 mientras que en el caso del artículo 5.1.f) del RGPD, se debe garantizar la confidencialidad e integridad. Como puede observarse, los dos artículos persiguen fines distintos, 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):
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 que nos ocupa, 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, mientras que 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 esta falta de medidas de seguridad hubiese sido detectada por la AEPD sin que se hubiera producido la pérdida de confidencialidad, únicamente habría sido sancionada por el artículo 32 del RGPD.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de confidencialidad, consecuencia de la deficiente aplicación de medidas técnicas u organizativas apropiadas para garantizar la confidencialidad de los datos y mediante el art. 32 del RGPD la deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento, ajenas a las que habrían posibilitado la materialización de la brecha de datos personales y cuya falta de implantación o de eficacia ha sido conocida por esta Agencia con motivo de la investigación llevada cabo. Estas medidas de seguridad deficientes infringen el RGPD, independientemente de que no se hubiera producido la pérdida de confidencialidad.

Dicho lo anterior, no se comparte el razonamiento expuesto en cuanto a que la AEPD sí ha aplicado este principio (non bis in ídem) en procedimientos como el PS/00027/2021 o el PS/00021/2021, toda vez que, es perfectamente admisible que la AEPD considere la vulneración de un determinado precepto en el convencimiento de que se ajuste más a los hechos que acontecen, sin que esta actuación pueda considerarse arbitraria, máxime cuando está debidamente motivada. Como ya se ha indicado, 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. Cuando la AEPD decide abrir un expediente sancionador, valora, a la vista de las circunstancias que concurren en el caso concreto, qué infracción o posibles infracciones del RGPD se habrían cometido.

El presente procedimiento sancionador se ha iniciado por la información y documentación obtenida tras el período de actuaciones previas de investigación, al inferirse de las mismas, una posible vulneración a la normativa en materia de protección de datos: el artículo 5.1 f) y el artículo 32 del RGPD.

Por las razones expuestas, no se entiende vulnerado el principio de non bis in ídem.

SÉPTIMA. SOBRE LA FALTA DE PROPORCIONALIDAD DE LA SANCIÓN.

En primer lugar, cabe recordar que las medidas correctivas de las que se dota a las Autoridades de Control se configuran en el RGPD como "poderes" esto es, como

potestades de actuación que, lógicamente, se aplicarán en atención a las circunstancias presentes en cada caso concreto.

Por otro lado, esta Agencia desea señalar lo que el Considerando 148 del RGPD indica sobre la posibilidad de imponer un apercibimiento:

"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante."

En atención a los términos en los que se pronuncia, el RGPD insta con carácter general a la imposición de multas y prevé que el apercibimiento sea la medida utilizada cuando la infracción sea leve- circunstancia que no sucede en este caso- o implique una carga desproporcionada cuando la infracción haya sido cometida por una persona física.

En este sentido, esta Agencia ha evaluado y motivado todas las circunstancias a que hace referencia el citado considerando 148 del RPGD (que no son otras que las del artículo 83.2 del RGPD) y toda vez que las infracciones en cuestión no son leves a efectos del RGPD, se considera conforme a Derecho imponer una multa en vez de dirigir un apercibimiento. Razón por la que se desestima la presente alegación.

En cuanto al principio de proporcionalidad, la STS, Sala 3ª, de 16 de diciembre de 2003 (Rec. 4996/98) ya señalaba que el principio de proporcionalidad de las sanciones exige que "*la discrecionalidad que se otorga a la Administración para la aplicación de la sanción se desarrolle ponderando en todo caso las circunstancias concurrentes, al objeto de alcanzar la debida proporcionalidad entre los hechos imputados y la responsabilidad exigida".* Principio de proporcionalidad que no se entiende vulnerado, considerándose proporcionada la sanción propuesta a la entidad, por los hechos probados y ponderadas las circunstancias concurrentes, que se detallan más adelante. En el presente caso, se han cometido dos conductas infractoras diferentes que han dado lugar a la vulneración de intereses jurídicos protegidos diferentes en cuyo caso, no cabe duda de que deben imputarse y sancionarse dos infracciones administrativas independientes

Esta Agencia desea señalar que el RGPD no obliga a que deban existir graves daños y/o perjuicios de la parte reclamante para constatar la existencia de infracción.

La naturaleza de la infracción, número de afectados, la existencia o no de daños y perjuicios, son todas cuestiones que se han tenido en cuenta y han sido debidamente motivadas a la hora de graduar la sanción a imponer a XFERA.

Ahora bien, frente a lo alegado, procede señalar varias cosas:

En primer lugar, el artículo 83.1 RGPD establece que las multas administrativas por las infracciones del RGPD deben ser "…*en cada caso individual efectivas, proporcionadas*

y disuasorias", indicando a continuación en el apartado 2 del citado precepto, que "*Las multas administrativas se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas*…" (el subrayado es nuestro). Estableciendo a continuación determinadas circunstancias a tener en cuenta.

Así, el cálculo del importe de las multas queda a decisión de la autoridad de control, con sujeción a las normas previstas en el RGPD.

En este contexto, el RGPD exige, como se ha señalado, que el importe de la multa sea en cada caso efectivo, proporcionado y disuasorio (artículo 83, apartado 1, del RGPD). Además, al fijar el importe de la multa, las autoridades de control tendrán debidamente en cuenta una lista de circunstancias que se refieren a las características de la infracción (su gravedad) o al carácter del autor (artículo 83, apartado 2, del RGPD).

Por último, el importe de la multa no excederá de los importes máximos previstos en el artículo 83, apartado 4, apartados 5 y 6, del RGPD.

Por lo tanto, la cuantificación del importe de la multa se basa en una evaluación específica realizada en cada caso, dentro de los parámetros previstos por el RGPD. Además, debe tenerse en cuenta que el cálculo de una multa no es un mero ejercicio matemático, siendo las circunstancias del caso específico los factores determinantes que conducen a la cantidad final, que puede ser, en todos los casos y para cada infracción, una cantidad distinta hasta el máximo legal.

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.

Por tanto, 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)

Recordemos en este punto lo manifestado por el TJUE en la sentencia dictada en el asunto C-683-21.

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

Reglamento de asegurar un elevado nivel de protección de esas personas en lo que respecta al tratamiento de los datos personales.

Asimismo, la reciente STJUE de 13 de febrero de 2025, en el asunto C-383/23, dispone que la imposición de una multa exige en el examen de cada caso particular de una serie de elementos previstos en el artículo 83 del RGPD, del que el volumen de negocios es un elemento más (ni el único ni el determinante), para imponer una multa que sea proporcional, disuasoria y efectiva y se refuerce, de esta forma, la protección de las personas físicas.

25 Así, en virtud del artículo 83, apartado 1, del RGPD, cada autoridad de control tiene que garantizar que las multas administrativas con arreglo al referido artículo 83 por las infracciones *del RGPD indicadas en sus apartados 4 a 6 sean, en cada caso individual, efectivas, proporcionadas y disuasorias.*
26 Más allá del cumplimiento de estos tres requisitos, el apartado 2 de dicho artículo 83 exige, para decidir la imposición de una multa administrativa y su importe, que la autoridad de control competente tenga debidamente en cuenta, en cada caso individual, una serie de elementos.
27 De conformidad con esta última disposición, entre esos elementos figuran, en particular, la naturaleza, gravedad y duración de la infracción, el número de interesados afectados y el nivel de los daños y perjuicios sufridos, la intencionalidad o negligencia en la infracción, las medidas adoptadas por el responsable o el encargado del tratamiento para paliar los daños y perjuicios sufridos, el grado de responsabilidad del responsable o del encargado del tratamiento y las categorías de datos personales afectados por la infracción.
28 Los citados elementos se refieren, bien al comportamiento de ese responsable o encargado, acusado de infringir determinadas disposiciones del RGPD, bien a las propias infracciones. Así pues, sirven para garantizar que cada una de dichas infracciones se aprecie sobre la base de todas las circunstancias individuales pertinentes y que se alcancen los objetivos perseguidos por el régimen sancionador contemplado en el RGPD.
29 Aunque estos elementos no hacen referencia al concepto de empresa, en el sentido de los artículos 101 TFUE y 102 TFUE, el Tribunal de Justicia ya ha declarado que solamente una multa que tenga en cuenta no solo todos los elementos que caractericen las infracciones del RGPD constatadas, sino también, en su caso, la capacidad económica real o material de su destinatario, reúne los tres requisitos establecidos en el artículo 83, apartado 1, del RGPD, a saber, ser a la vez efectiva, proporcionada y disuasoria. Pues bien, para apreciar estos requisitos, debe tenerse en cuenta si ese destinatario forma parte de una empresa en el sentido de los artículos 101 TFUE y 102 TFUE (véase, en este sentido, la sentencia de 5 de diciembre de 2023, Deutsche Wohnen, C 807/21, EU:C:2023:950, apartado 58).

En consecuencia, las alegaciones deben ser desestimadas.

Circunstancias invocadass:

-Naturaleza, gravedad y duración de la infracción.

A este respecto, procede señalar que estas circunstancias se tienen en cuenta para establecer el nivel de gravedad de las infracciones que se consideran cometidas, pero no operan como circunstancias agravante de acuerdo con las Directrices 04/2022 sobre el cálculo de las multas bajo el RGPD, según la cual la cuantía de la multa debe tener como punto de partida, tres elementos: el volumen de negocios en aquellos casos en los que el infractor sea una empresa, la categorización de las infracciones según su propia naturaleza (es decir, si se trata de una infracción del 83.4, 83.5 u 83.6 RGPD) y el nivel de gravedad de la infracción en cada caso concreto (de acuerdo con el artículo 83.2 a), b) y g). Pues bien, en este caso, se tiene en cuenta el elevado número de clientes de XFERA sobre los que se realizan operaciones de tratamiento referidas al tratamiento sobre el que se ha producido la brecha de datos personales: ***CANTIDAD.1 y de clientes que han resultado afectados por la brecha de datos personales: ***CANTIDAD.2.

Así, los resultados de la investigación apuntan a que la brecha afectó a un volumen aproximado de ***CANTIDAD.4 (…)*.”*

En el caso que nos ocupa, el tipo de datos que trata y que fueron afectados por la brecha y que XFERA parece desdeñar, supone un riesgo alto, en caso de vulnerarse su confidencialidad, de ser usados de modo fraudulento: suplantación de la identidad phishing, fraude financiero, etc.

Lo que se trata de poner en evidencia es que la vulneración de las infracciones se halla acrecentada y agravada por el número de afectados por el incidente, los daños y perjuicios provocados (pérdida irreversible de poder y control de los datos personales por los clientes).

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*”.

-De la ausencia de perjuicio para los interesados afectados por la brecha.

En cuanto al argumento de que no consta la existencia de perjuicio material o económico como resultado de la brecha de seguridad de XFERA, en primer lugar, esta Agencia desea reiterar que el RGPD no obliga a que deban existir graves daños y/o perjuicios de la parte reclamante para constatar la existencia de infracción, como en el presente caso.

Y en segundo lugar no es causa de justificación o exculpación suficiente, toda vez que los afectados se han visto desprovistos del control sobre sus datos personales, algunos han sido víctimas de phishing y en algunos casos, con cargos desconocidos en la factura del teléfono. En este caso la búsqueda en internet, por ejemplo, del nombre, apellidos de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, permita el acceso a otras

aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular. Esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

-Intencionalidad o negligencia en la sanción.

El hecho de que XFERA sea una empresa para cuya actividad realiza un constante y abundante manejo de datos personales, realizando tratamientos que implican un probable alto riesgo para los derechos y libertades de las personas físicas supone la exigencia de una diligencia mayor en la implantación de medidas para la protección de los datos personales que la que se pueda exigir a una pequeña empresa con menos recursos económicos y técnicos que XFERA y que realice un menor número de tratamientos, incluso esporádicos o accesorios.

Teniendo en cuenta que en la conducta de la entidad investigada concurre el elemento de culpabilidad, que es indispensable para poder exigir responsabilidad sancionadora, en este caso se concreta, además, en una muy grave falta de diligencia en la adopción de medidas adecuadas para la protección de los datos de carácter personal y para comprobar su cumplimiento como se ha puesto de manifiesto a lo largo del procedimiento.

Además, la falta de diligencia demostrada en la conducta infractora de la que se le responsabiliza debe calificarse de muy grave, pues datos de alta sensibilidad como el IBAN se encontraban en claro y sin cifrar. La entidad investigada está obligada en virtud del artículo 5.2 del RGPD a desplegar la actividad adecuada para cumplir los principios de protección de datos, por lo que aquí interesa, el de confidencialidad, y a estar en condiciones de demostrar su cumplimiento.

-Medidas adoptadas para paliar los daños y perjuicios sufridos por los interesados.

Como se ha indicado anteriormente, la entidad no habría adoptado medidas para impedir que terceros no autorizados explotaran la vulnerabilidad identificada.

-Infracciones anteriores cometidas por Xfera.

El considerando 148 del RGPD señala que:

“A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de

conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías."

Así pues, conforme al apartado e) del artículo 83.2. RGPD, en la determinación del importe de la sanción de multa administrativa no podrán dejar de valorarse todas aquellas infracciones anteriores del responsable o del encargado de tratamiento en aras a calibrar la antijuricidad de la conducta analizada o la culpabilidad del sujeto infractor.

Por tanto, las infracciones anteriores a la infracción objeto de examen más lejanas en el tiempo o menos próximas a la infracción actual sí deben ser tenidas en cuenta al decidir sobre la cuantía de la sanción, aunque como aclaran las Directrices sobre multas las autoridades podrán concederles menor transcendencia en la fijación del importe de la multa.

Además, una correcta interpretación de la disposición del artículo 83.2.e) RGPD no puede obviar la finalidad perseguida por la norma: decidir la cuantía de la sanción de multa administrativa en el caso individual planteado atendiendo siempre a que la sanción sea proporcional, efectiva y disuasoria.

En este caso, se han valorado adecuadamente y tenido en cuenta todas las circunstancias pertinentes, estableciéndose los importes de las multas en base a estas circunstancias, manteniendo al mismo tiempo, como se ha indicado, el carácter efectivo, disuasorio y proporcionado de la multa, que no supera el máximo legal aplicable.

Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que XFERA ha sido sancionada por la infracción de los artículos 5.1f) o 32 del RGPD. (Ej.: PS/00027/2021, PS/00448/2020, PS/00104/2020)

En el desarrollo de la actividad que le es propia, necesita de manera habitual tratar datos de carácter personal, lo que incide en la diligencia que le es exigible para el cumplimiento de los principios que presiden el tratamiento de datos de carácter personal y la calidad y efectividad de las medidas técnicas y organizativas que debe tener implementadas para garantizar el respeto de este derecho.

-Adhesión a códigos de conducta o a mecanismos de certificación aprobados.

Finalmente, en cuanto a la adhesión a códigos de conducta o a mecanismos de certificación aprobados de cara a reforzar el cumplimiento en materia de protección de datos, se ha de indicar que XEFERA aporta como Documento n.º 15 certificado del Sistema de Gestión de seguridad de la Información conforme con la ISO 27001 para los sistemas de información que soportan los servicios de comunicaciones móviles y de conectividad fija.

También aporta, como Documento n.º 16, certificado el Sistema de Gestión de seguridad de la Información conforme con la norma Privacidad de la información ISO

27701, igualmente referida al sistema de gestión de privacidad que da soporte a los servicios de comunicaciones móviles y servicios de conectividad fija.

Por tanto, ninguna de las dos certificaciones afectaría a la seguridad de la Aplicación VFR.

En definitiva, aunque la documentación aportada por XFERA puede reflejar una conducta positiva, no desvirtúa los hechos constatados.

Por último, resaltar que no ha aportado el informe pericial detallado en la carta de aceptación de encargo que se anexaba como Documento nº 13, relativo al análisis de las medidas de seguridad que pudiesen ser de interés en relación con este procedimiento.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de las infracciones que se declaran cometidas ni suponen causa de justificación o exculpación suficiente.

V

Obligación incumplida. Principio de integridad y de confidencialidad.

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

1. Los datos personales serán:

(…)

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

En relación con este principio, el Considerando 39 del referido RGPD señala que:

"[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Según las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679 del GT29 se produce una «violación de la confidencialidad» cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos; una «violación de la integridad»: cuando se produce una alteración no autorizada o accidental de los datos personales; y una «violación de la disponibilidad»: cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos .

El principio de confidencialidad e integridad, dentro del marco del RGPD, implica la obligación de garantizar que los datos personales se mantengan protegidos y

únicamente puedan ser accesibles o modificados por aquellos que tienen autorización para su tratamiento, con el fin legítimo previsto por el responsable del tratamiento.

En el caso que nos ocupa, de las actuaciones de investigación realizadas por la presente autoridad, se desprende una presunta vulneración del citado principio de confidencialidad. Dicha vulneración se manifiesta en el acceso no autorizado y exfiltración de datos personales de los clientes, lo que motivó la presentación por parte de estos, de distintas reclamaciones dirigidas a esta Agencia, relacionadas con la brecha de datos personales, al haber sido víctimas de phishing y en algunos casos, con cargos desconocidos en la factura del teléfono.

(…)

Todo ello constituye una vulneración de del principio de confidencialidad, establecido en el citado artículo 5.1.f) del RGPD.

En este sentido, no debe olvidarse, tal y como ha quedado expuesto en las actuaciones de investigación y de la información transmitida, que los atacantes accedieron y exfiltraron datos personales de ***CANTIDAD.4 (…).

(…). Este nivel de acceso aumenta el riesgo de uso indebido y fraude y pone de manifiesto que las medidas técnicas y organizativas adoptadas por el responsable no eran las apropiadas para garantizar la integridad y confidencialidad adecuada de los datos personales, en especial para la protección contra el tratamiento no autorizado o ilícito.

El art. 24 del RGPD sobre la responsabilidad del responsable del tratamiento, dispone en su apartado 1 que “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. (el subrayado es nuestro).

Por su parte, el Considerando 74 del RGPD declara que “*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas*”

Sobre este particular, cabe recordar la STJUE de 27 de febrero de 2025, asunto C-638/23, que determina en relación con la responsabilidad del responsable del tratamiento, lo siguiente:

> 32 (...) procede recordar que del considerando 74 del RGPD se desprende que el legislador de la Unión quiso que la responsabilidad que recae sobre el

responsable del tratamiento sea idéntica cualquiera que sea el tratamiento de datos personales que efectúe, ya sea por sí mismo o a través de un tercero, pero por su cuenta. El legislador de la Unión también quiso velar por que el responsable del tratamiento esté obligado a aplicar medidas oportunas y eficaces y pueda demostrar la conformidad de las actividades de tratamiento con dicho Reglamento, incluida la eficacia de las medidas en cuestión, que deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

33 En esta medida, el artículo 5, apartado 2, del RGPD consagra un principio de responsabilidad, en virtud del cual el responsable del tratamiento es responsable del cumplimiento de los principios relativos al tratamiento de datos personales enunciados en el apartado 1 de ese artículo 5, y establece que este debe ser capaz de demostrar que se respetan los referidos principios.

Y añade el Considerando 76 que "*La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto*"

Las Directrices WP248 del GT29, sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD, adoptadas el 4 de abril de 2017 y revisadas por última vez y adoptadas el 4 de octubre de 2017, definen los conceptos de "riesgo" y de "gestión del riesgo". Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias estimado en términos de gravedad y probabilidad. Por otra parte, la «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

Lo que implicará, por lo que aquí interesa, la aplicación de aquellos recursos, procedimientos y controles que pudieran ser necesarios para garantizar el cumplimiento del principio de confidencialidad, lo que no consta que se haya realizado.

En este sentido, la referida guía también recoge "*Como interpreta la Declaración WP218, hay que subrayar que abordar los riesgos que pudiera entrañar un tratamiento de datos para los derechos y libertades de las personas no puede limitarse a aplicar exclusivamente medidas de seguridad. Por lo tanto, la gestión de los riesgos de seguridad es una más de las actividades para la gestión de los riesgos para los derechos y libertades y se tiene que supeditar a esta última. Además, desde el punto de vista del RGPD, las medidas de mitigación han de estar orientadas a reducir el impacto y la probabilidad de que las brechas de datos personales afecten al interesado*" ·.

En consecuencia, se considera que los hechos acreditados son constitutivos de una infracción, imputable a la entidad investigada, por vulneración del artículo 5.1.f) del RGPD.

VI

Tipificación y calificación de la infracción

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. (…)"*

VII
Sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"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, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) 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;
b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42,
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo con lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 5.1 f) del RGPD, procede cuantificar la sanción que se propone, considerando para ello que la multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el

artículo 83.1 del RGPD.

Se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, así como del artículo 76.2 de la LOPDGDD anteriormente reproducidos.

Lo anterior implica de acuerdo con las Directrices 04/2022 sobre el cálculo de las multas bajo el RGPD que la cuantía de la multa debe tener como punto de partida, tres elementos: el volumen de negocios, la categorización de las infracciones según su propia naturaleza (es decir, si se trata de una infracción del 83.4, 83.5 u 83.6 RGPD) y el nivel de gravedad de la infracción en cada caso concreto (de acuerdo con el artículo 83.2 a), b) y g) y, en aquellos casos en los que el infractor sea una empresa, el volumen de negocios. En cualquier caso, la multa a imponer debe ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD

En este sentido, se considera, con carácter previo, el volumen de negocio de de XFERA, que en el ejercicio 2023 ascendió a 2.098.178.000 millones de euros.

En primer término, se tiene en cuenta la categoría de la infracción cometida, comprendida en el nivel superior del artículo 83 del RGPD, que la norma sanciona con la mayor gravedad en su apartado 5, castigando la conducta con una multa máxima de 20 millones de euros o, tratándose de una empresa, con una multa por una cuantía equivalente al 4% como máximo de su volumen de negocio anual. Según el citado precepto, al establecer el importe máximo aplicable debe optarse por el límite de mayor cuantía, de los dos fijados por la norma.

En este caso, tratándose de una empresa, cuyo volumen de negocio ascendió en el año 2023 a 2.098.178.000 millones de euros, el importe de la multa que procede imponer estará necesariamente situado entre 0,00 euros y 83.927.120 euros.

De acuerdo con los preceptos transcritos, a efectos de fijar el importe final de la sanción a imponer en el presente caso por la infracción del artículo 5.1.f) del RGPD de la que se responsabiliza a XFERA, tipificada en el artículo 83.5.a) del RGPD, se estiman concurrentes los siguientes factores:

Como elementos determinantes del nivel de gravedad de la infracción, se toman en consideración las circunstancias siguientes:

Artículo 83.2 a) RGPD*: "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";*

Conviene señalar que la vulneración del principio de confidencialidad en el presente caso involucra un conjunto de datos personales cuya naturaleza amplifica las implicaciones de la brecha de seguridad. Ello se desprende en la circunstancia de que se hayan visto afectados determinados datos personales como son nombre y apellidos, fecha de nacimiento, número de NIF, correo electrónico, números de teléfono, IBAN de la cuenta asociada y dirección física.

La combinación de este tipo de datos personales eleva significativamente el nivel de riesgo para los derechos y libertades de sus titulares y las implicaciones de la vulneración de la confidencialidad. Esto se debe a la circunstancia de que dicha combinación no solo aumenta la cantidad de información disponible para un actor malicioso, sino que también amplía el espectro de posibles abusos. Dado que no se trata de datos aislados o piezas individuales de información, sino de la exposición de un conjunto integrado de datos personales que cuando se combinan, pueden ser utilizados para construir un perfil completo y detallado de un individuo, lo cual puede permitir a un atacante realizar operaciones de fraude y suplantación de identidad con una mayor tasa de éxito.

Por último, no puede obviarse el número considerable de afectados por la brecha, dado que se ha constatado un impacto a ***CANTIDAD.2, lo que resalta tanto la escala del incidente como el volumen considerable de individuos cuyos derechos y libertades fueron comprometidos. Esta amplia afectación amplifica la gravedad de la infracción, dado que cada cliente afectado representa un potencial caso de fraude, suplantación de identidad, o pérdida financiera, multiplicando exponencialmente las repercusiones negativas del incidente.

Además, la infracción se ve agravada por el contexto en el que se produce, donde los individuos confían en la entidad para el manejo seguro de su información personal, habiéndose erosionado la confianza y expectativas de los afectados respecto al tratamiento de sus datos personales.

En cuanto a la duración de la brecha de datos personales, esta se extendió desde el 6 de marzo, fecha en la que aparecían eventos relacionados con una superación de los umbrales establecidos para determinar la capacidad máxima de consultas (logs) dentro del ecosistema del que forma parte la aplicación VFR, hasta el 28 ó 29 de marzo de 2023, fecha en la que el ataque es detectado a raíz de una revisión manual de los eventos del sistema por parte de un técnico de la entidad.

Artículo 83.2 b) RGPD: “*La intencionalidad o negligencia en la infracción”*

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 entidad reclamada 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 prevenciones legales al respecto. [Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)].

Tal y como ha quedado expuesto en las actuaciones de investigación y de la información transmitida, los atacantes accedieron a datos personales de los clientes. Además, los datos de IBAN no estaban cifrados, anonimizados o protegidos de forma ininteligible, lo que evidencia una falta de diligencia grave por parte de Xfera en el cumplimiento de sus obligaciones

Este nivel de acceso aumenta el riesgo de uso indebido y fraude y pone de manifiesto que las medidas técnicas y organizativas adoptadas por el responsable no eran las apropiadas para garantizar la integridad y confidencialidad adecuada de los datos personales, en especial para la protección contra el tratamiento no autorizado o ilícito.

Dicha circunstancia refleja una omisión palmaria del responsable en el deber de cuidado hacia la protección de los datos de sus clientes, lo que refuerza y amplifica la gravedad de la infracción.

Artículo 83.2 g) RGPD*: las categorías de los datos de carácter personal afectados por la infracción;*

Toda vez que se han visto afectados datos como el IBAN de la cuenta asociada cuya exposición aumenta el riesgo de uso indebido y fraude lo que amplifica la gravedad de la infracción dado que existió para cada cliente, riesgo de fraude, suplantación de identidad, o pérdida financiera, multiplicando exponencialmente las repercusiones negativas del incidente. ***(…).***

Se tienen en cuenta como circunstancias agravantes:

Artículo 83.2.e) RGPD: "*Toda infracción anterior cometida por el responsable o el encargado del tratamiento."*

Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que la entidad investigada ha sido sancionada por la infracción del artículo 5.1f) del RGPD (Ej.: PS/00027/2021, PS/00448/2020, PS/00104/2020)

Artículo *76.2 b) LOPDGDD: "La vinculación de la actividad del infractor con la realización de tratamientos de datos personales"*

La actividad empresarial de la entidad investigada exige un continuo tratamiento de datos de carácter personal. La empresa opera en un sector donde la confianza y la seguridad de la información resulta fundamental, además el uso de tecnología avanzada para ofrecer servicios eficientes no les resulta ajena, y por tal motivo tiene la responsabilidad garantizar con mayor rigurosidad los principios de protección de datos respecto a la información que gestiona en virtud de dicha actividad.

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa es de 2.500.000 euros por infracción del artículo 5.1 f) del RGPD.

VIII

Obligación incumplida. Seguridad del tratamiento.

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

"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 Considerando 74 del RGPD, anteriormente reproducido, establece:

"*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas."*

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

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

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

En este mismo sentido el considerando 83 del RGPD señala que:

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

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

De las actuaciones de investigación desarrolladas por la presente autoridad, se desprende una posible insuficiencia de medidas de seguridad existentes, que puede inferirse fácilmente del hecho de que:

- (…).

Por tanto, de lo que antecede se desprende que las medidas de seguridad técnicas y organizativas implantadas por la entidad no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los datos de los clientes.

En consecuencia, se considera que los hechos acreditados son constitutivos de una infracción, imputable a la entidad investigada, por vulneración del artículo 32 RGPD, toda vez que, si bien la entidad investigada tomó medidas reactivas, dichas acciones llegaron como respuesta a una vulnerabilidad ya explotada, en lugar de como parte de una estrategia proactiva de gestión de riesgos.

IX
Tipificación y calificación de la infracción

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."

X
Sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"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, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) 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;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42,
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo con lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 32 del RGPD, procede cuantificar la sanción que se propone, considerando para ello que la multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD.

Se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, así como del artículo 76.2 de la LOPDGDD anteriormente reproducidos.

Lo anterior implica de acuerdo con las Directrices 04/2022 sobre el cálculo de las multas bajo el RGPD que la cuantía de la multa debe tener como punto de partida, tres elementos: el volumen de negocios, la categorización de las infracciones según su propia naturaleza (es decir, si se trata de una infracción del 83.4, 83.5 u 83.6 RGPD) y el nivel de gravedad de la infracción en cada caso concreto (de acuerdo con el artículo 83.2 a), b) y g) y, en aquellos casos en los que el infractor sea una empresa, el volumen de negocios. En cualquier caso, la multa a imponer debe ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD

En este sentido, se considera, con carácter previo, el volumen de negocio de XFERA, que en el ejercicio 2023 ascendió a de 2.098.178.000 €.

En primer término, se tiene en cuenta la categoría de la infracción cometida, comprendida en el nivel regulado en el artículo 83.4 del RGPD, que la norma sanciona con una multa máxima de 10 millones de euros o, tratándose de una empresa, con una multa por una cuantía equivalente al 2% como máximo de su volumen de negocio anual. Según el citado precepto, al establecer el importe máximo aplicable debe optarse por el límite de mayor cuantía, de los dos fijados por la norma.

En este caso, teniendo en cuenta el volumen de negocio de XFERA, el importe de la multa que procede imponer estará necesariamente situado entre 0,00 euros y 41.963.560 euros.

De acuerdo con los preceptos transcritos, a efectos de fijar el importe final de la sanción a imponer en el presente caso por la infracción del artículo 32 del RGPD de la que se responsabiliza a XFERA, tipificada en el artículo 83.4.a) del RGPD, se estiman concurrentes los siguientes factores:

1. Como elementos determinantes del nivel de gravedad de la infracción, se toman en consideración las circunstancias siguientes:

Artículo 83.2 a) RGPD*: "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";*

Los hechos determinan el incumplimiento de una obligación básica establecida por el RGPD, como es el establecimiento de las medidas de seguridad adecuada para la protección de los datos personales.

Asimismo, en cuanto al número de interesados afectados, según XFERA el número aproximado de personas físicas sobre las que se realizan operaciones de tratamiento referidas al tratamiento sobre el que se ha producido la brecha de datos personales asciende a ***CANTIDAD.1. Por tanto, la ausencia de medidas de seguridad afectó a todos estos clientes de la entidad investigada Esta amplia afectación amplifica la gravedad de la infracción, dado que existió para cada cliente, riesgo de fraude, suplantación de identidad, o pérdida financiera, multiplicando exponencialmente las repercusiones negativas del incidente.

Artículo 83.2 b) RGPD: "*La intencionalidad o negligencia en la infracción"*

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 entidad reclamada 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 prevenciones legales al respecto. [Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)].

(…).

Dicha circunstancia refleja una omisión palmaria en el deber de cuidado hacia la protección de los datos de sus clientes, lo que refuerza y amplifica la gravedad de la infracción y justifica, en consecuencia, la concurrencia de esta agravante.

En calidad de agravantes se tienen en cuenta:

Artículo 83.2.e) RGPD: "*Toda infracción anterior cometida por el responsable o el encargado del tratamiento."*

Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que la entidad investigada ha sido sancionada por la infracción del artículo 32 del RGPD. (Ej: PS/00237/2019, PS/00448/2020, PS/00104/2020)

Artículo *76.2 b) LOPDGDD: "La vinculación de la actividad del infractor con la realización de tratamientos de datos personales"*

La actividad empresarial de la entidad investigada exige un continuo tratamiento de datos de carácter personal. Por otra parte, la empresa opera en un sector donde la confianza y la seguridad de la información resulta fundamental, además el uso de tecnología avanzada para ofrecer servicios eficientes no les resulta ajena, y por tal motivo tiene la responsabilidad de garantizar con mayor rigurosidad los principios de protección de datos respecto a la información que gestiona en virtud de dicha actividad. La naturaleza de dicha actividad exigía una mayor rigurosidad en la adopción de las medidas de seguridad, exigencia que no fue materializada en el caso que nos ocupa.

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa es de 1.500.000 euros por infracción del artículo 32 del RGPD.

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

PRIMERO: IMPONER a XFERA MÓVILES, S.A.U., con NIF A82528548,

-por la infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción, en el artículo 72.1 a) de la LOPDGDD, una multa de 2.500.000 euros.

- por la infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción, en el artículo 73 f) de la LOPDGDD, una multa de 1.500.000 euros.

SEGUNDO: NOTIFICAR la presente resolución a XFERA MÓVILES, S.A.U.

TERCERO: 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 (BIC/Código SWIFT: CAIXESBBXXX)***, 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. La publicación se realizará una vez la resolución sea firme en vía administrativa.

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 Presidencia 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://sedeaepd.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.

938-180725

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos