- **Expediente nº.: EXP202213023**

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por **ORANGE ESPAGNE, S.A.U.** (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 22 de octubre de 2024, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 22 de octubre de 2024, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202213023, en virtud de la cual se imponía a **ORANGE ESPAGNE, S.A.U.**:

-por una infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) de dicha norma, multa administrativa de cuantía 200.000 euros (doscientos mil euros).

- por una infracción del artículo 25 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 1.000.000 euros (un millón de euros).

- ORDENAR a ORANGE ESPAGNE, S.A.U., con NIF A82009812, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 6 meses, notifique a esta Agencia las medidas que ha adoptado para garantizar que la solicitud de duplicado se presenta por el titular del número de teléfono, sea cual sea el procedimiento utilizado para su emisión.

SEGUNDO: Dicha resolución, que fue notificada a la parte recurrente en fecha 23 de octubre de 2024, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

TERCERO: Como hechos probados del citado procedimiento sancionador, PS/00332/2023, quedó constancia de los siguientes:

HECHOS PROBADOS

PRIMERO: Consta que, en fecha 15 de diciembre de 2022 se realizó un duplicado de la tarjeta SIM titularidad de la parte reclamante, sin que lo hubiera solicitado, en el establecimiento titularidad de "TOWER PHONE, S.L.," ubicado en la calle ******DIRECCIÓN.1*** de Madrid, que actúa como franquicia de **ORANGE**, según consta en el contrato de franquicia de fecha 1 de abril de 2022.

De este modo, en el contrato de franquicia de fecha 1 de abril de 2022 aportado por **ORANGE** con la entidad TOWER PHONE S.L.U., se puede observar:

"*Antecedentes:*

I. Que forma parte de la actividad y objeto social de ORANGE la prestación y comercialización de diversos servicios de telecomunicaciones, comunicaciones electrónicas y para la sociedad de la información.

II. Que ORANGE ESPAGNE S.L.U., en desarrollo de su objeto social comercializa sus servicios y ha implantado su red comercial en el tráfico mercantil bajo las marcas y demás signos distintivos que le son propios o cuyos usos de marca está legitimado a ceder, estando interesada en designar franquiciados, (…)."

(…).

*IV**. (…).***

*V**. (…).***

Asimismo, en el objeto del contrato se puede observar:

(…).

(…).

SEGUNDO: **ORANGE** es la responsable de los tratamientos de datos referidos en el presente procedimiento, toda vez que conforme a la definición del artículo 4.7 del RGPD es quién determina la finalidad y medios de los tratamientos realizados.

En la cláusula Vigesimosegunda, relativa al tratamiento de datos personales, se aprecia:

"En virtud del presente contrato, el FRANQUICIADO en su condición de encargado de tratamiento, llevará a cabo el tratamiento de datos personales necesario para la correcta prestación de los servicios objeto de este contrato."

TERCERO: Consta que, para solicitar el duplicado de la tarjeta SIM, **ORANGE** tiene implementado un sistema automático de validación del documento de identidad, pero que, en algunos casos ***(…)*** de la persona que solicita el duplicado de dicha tarjeta SIM, ***(…)***.

CUARTO: **ORANGE** ha afirmado que, en el momento de la contratación del duplicado de tarjeta SIM de la parte reclamante, "*se siguió el protocolo establecido por esta mercantil pasando un documento de identidad por el sistema de verificación* ***(...)***."

(…).

*En cuanto a la cuestión relativa a si el sistema de **(...)** comprueba la correspondencia de número de documento y nombre del titular del documento con los datos del solicitante del trámite, **(…).***

*Por ello, por regla general, el sistema **(...)** sí valida el nombre del titular del documento de identidad con la información del solicitante del trámite, **(…).***

QUINTO: ***(…)***.

SEXTO: **ORANGE** ha reconocido que el duplicado de la tarjeta SIM de la parte reclamante se había producido por una irregularidad de agentes que trabajaban en la tienda en la que se produjo el duplicado de la tarjeta SIM, ***(…)***.

SÉPTIMO: **ORANGE** ha manifestado, en su escrito de fecha 30 de marzo de 2023, que ha dado a sus empleados las siguientes instrucciones acerca de cómo proceder con la utilización del sistema de validación del DNI, y son las siguientes:

- es de obligado cumplimiento no realizar un cambio o duplicado de tarjeta SIM a una persona distinta del titular (o administrador o autorizado de la empresa que conste en sistemas). La persona que vaya a realizar un duplicado deberá aportar un documento válido de identidad (conforme a protocolo), el cual siempre será validado. (…)

-si en el momento de la solicitud no funcionara el sistema, el agente deberá abrir una incidencia y emplazar al cliente a que vuelva al día siguiente.

-el agente que gestione una solicitud de duplicado deberá solicitar la documentación de identidad, ***(…)***.

-en los casos en los que el documento de identidad ***(…)***.

OCTAVO: **ORANGE** ha manifestado en su escrito de alegaciones de fecha 21 de diciembre de 2023, que tiene implementadas las siguientes medidas en los supuestos de solicitud de duplicados de tarjeta SIM:

-Desde el 12 de agosto de 2022 ***(…)***.

-Desde el 12 de agosto de 2022 ***(…)***.

-Desde abril de 2021, **ORANGE** ha ido limitando los canales desde los cuales se puede solicitar un duplicado de tarjeta SIM ***(…).***

NOVENO: **ORANGE** ha manifestado en su escrito de contestación al traslado de la reclamación, de fecha 30 de enero de 2023, así como en su escrito de contestación al requerimiento, de fecha 30 de marzo de 2023, y de alegaciones al acuerdo de inicio del presente expediente sancionador, de fecha 21 de diciembre de 2023, que habría adoptado las siguientes medidas para prevenir la comisión de fraudes derivados de la suplantación de agentes y/o empleados de **ORANGE**:

- con fecha 28 de diciembre de 2022, y con anterioridad a la notificación del presente requerimiento, se habría dado traslado desde la Escuela de Comerciales a todo el

canal de distribución a los puntos de venta una píldora formativa obligatoria con el fin de ayudar y concienciar a los equipos comerciales del riesgo de captar a comerciales para realizar duplicados físicamente desde los puntos de venta."

-- Se habría impulsado la difusión a todo el canal de distribución de una píldora formativa con el objetivo de concienciar a los trabajadores de la problemática existente y de la obligatoriedad de cumplir con todos los procedimientos y políticas de identificación de clientes.

-Se habría puesto en marcha la implantación de un doble factor de identificación, cuyo proyecto piloto ya se encuentra implantado, estando en fase de testeo.

-se habría puesto en marcha un proyecto ***(…).***

-se habría puesto en marcha una herramienta del Grupo de Análisis de Riesgos, que permite que se generen alertas en caso de posible detección de contrataciones irregulares, y que en el caso de duplicados de tarjeta SIM actuarían de la siguiente manera:

(…).

(…).

- Desde el 14 de diciembre de 2022, según manifiesta **ORANGE** en su escrito de alegaciones al acuerdo de inicio del presente expediente sancionador, habría procedido a la suspensión cautelar de la opción que permite a los agentes de punto de venta, ***(…)***, sin poder así atender ningún tipo de excepción.

DÉCIMO: En relación con el supuesto que ha motivado este expediente sancionador, **ORANGE** ha manifestado, en su escrito de alegaciones al presente expediente sancionador de fecha 21 de diciembre de 2023, que habría realizado las siguientes actuaciones:

-Se ha interpuesto una denuncia contra los agentes responsables.

-Los agentes implicados fueron dados de baja del establecimiento.

DÉCIMO PRIMERO: Consta que, en la denuncia presentada por la entidad TOWER PHONE, S.L., en fecha 12 de enero de 2023, se define el concepto de SIM SWAPPING de la siguiente manera:

"*El SIM Swapping es un ciberataque que consiste en suplantar la identidad de una persona ante su compañía de servicios telefónicos y pedir un duplicado de la tarjeta SIM de su teléfono móvil para con ello, acudir a su banca online y operar con la misma, recibiendo los SMS con el código de confirmación de operaciones bancarias en esa nueva SIM, procediendo a desviar el dinero de la cuenta corriente de la persona suplantada hacia otra propiedad de los delincuentes.*

La víctima, tal y como sucede en el presente supuesto, solo se entera de la situación cuando deja de tener cobertura en su teléfono móvil y por mucho que reinicia el

dispositivo o intenta buscar cobertura no lo consigue ya que, al entrar en funcionamiento la nueva SIM duplicada que los ciberdelincuentes piden a la compañía de servicios telefónicos, la SIM que está dentro del teléfono de la víctima deja de funcionar."

DÉCIMO SEGUNDO: Consta que en la denuncia presentada por TOWER PHONE S.L., se recoge que "se interpone denuncia contra ***A.A.A.*** con NIE: (…) por posible delito de:

(…)

Asimismo, consta que al hablar del concepto de SIM Swapping se recoge:

"*En primer lugar, es importante explicar en qué consiste los hechos aquí denunciados (SIM Swapping) llevados a cabo por el denunciado* ***B.B.B.*** *en, al menos, los días 14, 17 y 21 de diciembre de 2022 en su centro de trabajo, el punto de venta Orange ubicado en el* ******ESTABLECIMIENTO.1*** *de Madrid (****DIRECCIÓN.1** *Madrid*)"

(…)

En el apartado cuarto de la denuncia, relativo a los Hechos denunciados recoge:

"En fechas recientes, mi representada ha tenido conocimiento de los hechos que pasamos a detallar a continuación, los cuales, han sido debidamente verificados y contrastados con los respectivos departamentos internos de la empresa, por medio de la emisión de informe y achacados al denunciado.

Se adjunta Informe Investigación interno con sus documentos adjuntos elaborado y suscrito por el Responsable de tienda situada en ******DIRECCIÓN.1*** Madrid, propiedad de Tower Phone, S.L., (…). Dichos anexos del informe de investigación interna son los siguientes:

Anexo 1: documentación justificativa horario laboral de ***A.A.A.*** en fecha 6 de octubre de 2022 (primera suplantación).

Anexo 2: documentación justificativa horario laboral de ***A.A.A.*** en fecha 7 de octubre de 2022 (segunda suplantación).

Anexo 3: documentación justificativa horario laboral de ***A.A.A.*** en fecha 13 de octubre de 2022 (tercera suplantación)

Anexo 4: documentación justificativa horario laboral de ***A.A.A.*** en fecha 3 de noviembre de 2022 (cuarta suplantación)

Anexo 5: documentación justificativa horario laboral de ***A.A.A.*** en fecha 15 de noviembre de 2022 (quinta suplantación)

EN PRIMER LUGAR, mi representado tuvo conocimiento de los hechos aquí denunciados por primera vez en fecha 20 de octubre de 2022, cuando acude a la tienda ORANGE sita en ******DIRECCIÓN.1*** de Madrid (…) alertando que hace unos días

vino a la tienda y que el mismo día le llamaron supuestamente de ORANGE. La consulta en la tienda se trataba de una factura impagada, y la llamada correspondía con la visita a la tienda y la factura impagada para cobrársela por tarjeta bancaria. Tras varios intentos fallidos con su tarjeta se puso en contacto con la clienta un chico ***(…)*** y le comentó que al ser paisanos era una estafa, que no hiciese caso, y que esas informaciones de clientes las recibían a través de las tiendas. Ya desde el primer momento, la clienta acusó directamente a ***A.A.A.*** (…) a lo cual se manda un correo a la supervisora para que tuvieran constancia de estos fraudes. (…)

(…)

EN SEGUNDO LUGAR, en fecha 16 de noviembre de 2022, llaman al responsable de la tienda de ORANGE (situado en la calle ******DIRECCIÓN.1***, Madrid) desde la tienda de ORANGE de ***(...)***, Madrid, indicando que el pasado día 15 de noviembre de 2022 a las 20:45 horas se había realizado un duplicado de tarjeta a la clienta ***C.C.C.*** utilizando el código del punto de venta correspondiente a la tienda ORANGE sita en ******DIRECCIÓN.1*** de Madrid.

Ante dichos hechos, el responsable de la tienda ORANGE de ******DIRECCIÓN.1*** pregunta al personal de tienda si habían realizado un cambio de tarjeta SIM el día anterior ya que en nuestro sistema de facturación no aparecía como facturado y se comprobó que la tarjeta SIM que se había utilizado estaba en el stock de la tienda. El personal comentó que no lo habían realizado y no tenían constancia. Al tener cámaras en la tienda se revisa el video del día de los hechos (15 de noviembre de 2023) donde se observa que a la hora donde se realizaba el duplicado de tarjeta se encuentran trabajando (…) y ***A.A.A.*** está en el ordenador de la caja al parecer hablando por teléfono con un auricular.

(…)

Dada la gravedad de los hechos, se remite ese mismo día toda la información a la supervisora de ORANGE y se manda un correo informativo de lo sucedido.

(…)

Posteriormente, en fecha 18 de noviembre, se responde el mismo por parte de la compañía telefónica ORANGE donde se le informa a esta parte de que para dicho trámite se ha utilizado documentación y firma de otra persona (…). Igualmente, se confirma a esta parte que dicha persona acudió a realizar un duplicado de tarjeta el día anterior al del fraude con el trabajador ***A.A.A.*** en la tienda ORANGE sita ******DIRECCIÓN.1***, y está facturado correctamente.

(…)

Cabe destacar que, al realizar el duplicado de tarjeta, se anula la que actualmente consta en el sistema y se sustituye por una nueva invalidando en mismo momento la tarjeta anterior normalmente se realizan cuando la tarjeta actual por ejemplo no funciona, el cliente ha perdido el teléfono móvil o se lo han robado. EL PROTOCOLO QUE SE TIENE QUE SEGUIR PARA HACER UN DUPLICADO es con el cliente presencial en la tienda y con su documento original y en vigor ya que debemos

escanear el documento para su validación y asegurarnos que es el titular de la línea el que realiza el cambio de la tarjeta SIM.

(…)

EN TERCER LUGAR y como consecuencia del fraude anteriormente detallado, esta parte solicita a ORANGE toda la información disponible para poder proceder a suspender o retirar de forma laboral al sospechoso ***A.A.A.*** de la tienda, y para ello esta parte necesitaba que su departamento de Ciberseguridad asegurara cuantos duplicados desde la tienda de ******DIRECCIÓN.1*** se han realizado siendo Fraudes, horario de tales y la IP que realizó ese duplicado. Esta IP es especialmente relevante ya que nos asegura que se realizó desde la tienda, y no desde otro ordenador externo o pc autorizado.

Esta parte, recibió confirmación por parte de ORANGE donde se informaba de los siguientes duplicados, todos ellos realizados con la IP ******IP.1*** correspondiente a los ordenadores de la Tienda Orange calle ******DIRECCIÓN.1***:

1. FRAUDE DUPLICADO TARJETA SIM (SIM SWAPPING) EN FECHA 06-10-2022, 20:42 HORAS EN EL PUNTO DE VENTA TIENDA ORANGE CALLE ******DIRECCIÓN.1***, MADRID.

En fecha 6 de octubre de 2022 a las 20:42 horas, se produjo un duplicado de la tarjeta SIM (…), número de IMSI (…) y perteneciente al número de móvil (…) propiedad de cliente de ORANGE (…) con DNI (…). Según la geolocalización de los IMEIS de los terminales utilizados para el duplicado de la SIM, la suplantación se produjo en la tienda ORANGE calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada. Para acreditar dicha geolocalización, esta parte va a oficiar a la comercializadora ORANGE para que aporte dicho informe.

Una vez se ha corroborado que el duplicado se llevó a cabo en la tienda ORANGE Calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada, los cuadrantes horarios que se han adjuntado en el informe de investigación interna (Anexo 1) muestran que en la franja horaria (06/10/2022) a las 20:42 horas) que se produjo el duplicado el único trabajador que estaba trabajando en dicha tienda era el denunciado. De esta manera, se puede confirmar al 100% que ***A.A.A.*** estaba en su correspondiente centro de trabajo (punto de venta) en las fechas y horas en que se produjeron dicho duplicado.
(…)

2. FRAUDE DUPLICADO TARJETA SIM (SIM SWAPPING) EN FECHA 07-10-2022, 20:36 HORAS EN EL PUNTO DE VENTA TIENDA ORANGE CALLE ******DIRECCIÓN.1***, MADRID.

En fecha 7 de octubre de 2022 a las 20:36 horas, se produjo un duplicado de la tarjeta con número de SIM (…), número de IMSI (…) y perteneciente al número de móvil (…) propiedad del cliente de ORANGE (…) con DNI (…). Según la geolocalización de los IMEIS de los terminales utilizados para el duplicado de la tarjeta SIM, la suplantación se produjo en la tienda ORANGE Calle ******DIRECCIÓN.1*** de Madrid propiedad de mi

representada. Para acreditar dicha geolocalización, esta parte va a oficiar a la comercializadora ORANGE para que aporte dicho informe.

Una vez se ha corroborado que el duplicado se llevó a cabo en la tienda ORANGE Calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada, los cuadrantes horarios que se han adjuntado en el informe de investigación interna (Anexo 2) muestran que en la franja horaria (07/10/2022) a las 20:36 horas que se produjo el duplicado el único trabajador que estaba trabajando en dicha tienda era el denunciado. De esta manera, se puede confirmar al 100% que ***A.A.A.*** estaba en su correspondiente centro de trabajo (punto de venta) en las fechas y horas en que se produjeron dicho duplicado.
(…)

3. FRAUDE DUPLICADO TARJETA SIM (SIM SWAPPING) EN FECHA 13-10-2022 18:43 HORAS EN EL PUNTO DE VENTA TIENDA ORANGE CALLE ******DIRECCIÓN.1*** MADRID.

En fecha 13 de octubre de 2022 a las 18:43 horas, se produjo un duplicado de la tarjeta con número SIM (…), número de IMSI (…), y perteneciente al número de móvil (…), propiedad del cliente (…) con DNI (…). Según la localización de los IMEIS de los terminales utilizados para el duplicado de la SIM, la suplantación se produjo en la tienda ORANGE calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada. Para acreditar dicha geolocalización, esta parte va a oficial a la comercializadora ORANGE para que aporte dicho informe.

Una vez se ha corroborado que el duplicado se llevó a cabo en la tienda Orange Calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada, los cuadrantes horarios que se han adjuntado en el informe de investigación interna (Anexo 3) muestran que en la franja horaria (13/10/2022) a las 18:43 horas que se produjo el duplicado el único trabajador que estaba trabajando en dicha tienda era el denunciado. De esta manera, se puede confirmar al 100% que ***A.A.A.*** estaba en su correspondiente centro de trabajo (punto de venta) en las fechas y horas en que se produjeron dicho duplicado.

(…)

4. FRAUDE DUPLICADO TARJETA SIM (SIM SWAPPING) EN FECHA 03-11-22 20:16 HORAS EN EL PUNTO DE VENTA TIENDA ORANGE CALLE ******DIRECCIÓN.1***, MADRID.

En fecha 3 de noviembre de 2022 a las 20:16 horas, se produjo un duplicado de la tarjeta con numero SIM (…), numero de IMSI (…) y perteneciente al número de móvil (…), propiedad del cliente de ORANGE (…) con DNI (…). Según la geolocalización de los IMEIS de los terminales utilizados para el duplicado de la SIM, la suplantación se produjo en la tienda Orange Calle ******DIRECCIÓN.1*** de Madrid propiedad de mi representada. Para acreditar dicha geolocalización, esta parte va a oficiar a la comercializadora Orange para que aporte dicho informe. Cabe destacar que dicho fraude fue alertado por Orange a mi representado en fecha 21 de noviembre de 2022.
(…)

Una vez se ha corroborado que el duplicado se llevó a cabo en la tienda Orange Calle ***DIRECCIÓN.1*** de Madrid propiedad de mi representada, los cuadrantes horarios que se han adjuntado en el informe de investigación interna (Anexo 4) muestran que en la franja horaria (03/11/2022) a las 20:16 horas que se produjo el duplicado el único trabajador que estaba trabajando en dicha tienda era el denunciado. De esta manera, se puede confirmar al 100% que ***A.A.A.*** estaba en su correspondiente centro de trabajo (punto de venta) en las fechas y horas en que se produjeron dicho duplicado.

(…)

5. FRAUDE DUPLICADO TARJETA SIM (SIM SWAPPING) EN FECHA 15-11-2022, 20:16 HORAS EN EL PUNTO DE VENTA TIENDA ORANGE CALLE ***DIRECCIÓN.1***, MADRID.

En fecha 15 de noviembre de 2022 a las 20:46 horas, se produjo un duplicado de la tarjeta con Número SIM (…), Número de IMSI: (…) y perteneciente al número de móvil (…), propiedad del cliente de Orange (…) con DNI: (…). Según la geolocalización de los IMEIS de los terminales utilizados para el duplicado de la SIM, la suplantación se produjo en la tienda Orange Calle ***DIRECCIÓN.1*** de Madrid propiedad de mi representada. Para acreditar dicha geolocalización, esta parte va a oficiar a la comercializadora Orange para que aporte dicho informe.

Una vez se ha corroborado que el duplicado se llevó a cabo en la tienda Orange Calle ***DIRECCIÓN.1*** de Madrid propiedad de mi representada, los cuadrantes horarios que se han adjuntado en el informe de investigación interna (Anexo 5) muestran que en la franja horaria (15/11/2022) a las 20:46 horas que se produjo el duplicado el único trabajador que estaba trabajando en dicha tienda era el denunciado. De esta manera, se puede confirmar al 100% que ***A.A.A.*** estaba en su correspondiente centro de trabajo (punto de venta) en las fechas y horas en que se produjeron dicho duplicado.

(…)

"*SEXTO,- Los hechos narrados pueden ser constitutivos de un:*

- POSIBLE DELITO DE ESTAFA CON MEDIOS ELECTRÓNICOS. (248.2 CP)

- Y/O POSIBLE DELITO DE HURTO (234 CP) Y/O POSIBLE APROPIACION INDEBIDA (235 CP Y SIGUIENTES)

- Y/O POSIBLE SUPLANTACIÓN DE IDENTIDAD CON USURPACIÓN DEL ESTADO CIVIL (401 CP).

- Y/O POSIBLE DELITO DE INTRUSIÓN INFORMÁTICA E INTERCEPTACIÓN DE TRASMISIONES DE DATOS INFORMÁTICOS (197 BIS CP)"

(…)

DÉCIMO TERCERO: **ORANGE** ha presentado en su escrito de alegaciones al acuerdo de inicio del presente expediente sancionador, de fecha 21 de diciembre de 2023, un “INFORME RGPD. OPINION DE AUDITORÍA. APLICACIÓN DE PRINCIPIOS DE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO”, fechado el día 18 de diciembre de 2023, y en las conclusiones se puede observar:

“***(…)”***

DECIMO CUARTO: **ORANGE** ha presentado en su escrito de alegaciones al acuerdo de inicio del presente expediente sancionador, un documento titulado “Procedimiento. Protección de Datos desde el diseño y por defecto”, con una versión inicial de fecha 04/04/2018, y, en su versión 2.0 de fecha 18 de noviembre de 2019, se puede observar en el apartado 4:

“4. Protección de Datos desde el Diseño

En cumplimiento con lo manifestado en la Guía de Privacidad desde el diseño publicada por la AEPD, **ORANGE** tiene la obligación de adoptar estrategias de diseño de privacidad orientadas a aplicar las medidas técnicas y organizativas que resulten apropiadas desde la primera fase de desarrollo de un sistema de información o de un nuevo proyecto o servicio que implique tratamiento de datos, y durante toda la ejecución del mismo, así como verificar y gestionar el control sobre la recogida, uso y divulgación de los datos personales tratados desde la primera fase de tratamiento de datos personales.

(…):

(…).

5. Protección de datos por defecto.

(…).

6. Implementación de medidas apropiadas

(…).

7. Verificación de cumplimiento

(…):

(…)

TERCERO: La parte recurrente ha presentado en fecha 25 de noviembre de 2024, en esta Agencia Española de Protección de Datos, recurso de reposición, fundamentándolo, básicamente, en:

1.- PREJUDICIALIDAD PENAL.

2.- SOBRE EL SUPUESTO DE HECHO.

i) Sobre la consideración de la tarjeta SIM como dato personal

ii) Sobre la realización de operaciones bancarias

iii) Sobre la relación de los autores del hecho delictivo con ORANGE

3.- SOBRE LA ACTUACION DELICTIVA DE LOS AGENTES.

4.- INEXISTENCIA DE FALTA DE LEGITIMACION EN EL TRATAMIENTO DE DATOS PERSONALES DE ORANGE.

5.- DE LA CORRECTA IMPLEMENTACION DE LA PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO.

i) Sobre el análisis de riesgos para los derechos y libertades

6.- SOBRE LA EXISTENCIA DE UN CONCURSO DE INFRACCIONES.

7.- SOBRE LA INADMISIBILIDAD DE LA RESPONSABILIDAD OBJETIVA.

8.- SOBRE LAS MEDIDAS ADOPTADAS E IMPLEMENTADAS POR ORANGE.

I) Medidas implementadas por ORANGE para prevenir la comisión de fraudes derivados de la suplantación de identidad de su cliente.

II) Medidas implementadas por ORANGE para prevenir la comisión de fraudes derivados de la suplantación de agentes y/o empleados de ORANGE.

9.- SOBRE LA FALTA DE PROPORCIONALIDAD DE LA SANCIÓN PROPUESTA.

FUNDAMENTOS DE DERECHO

I
Competencia

Es competente para resolver el presente recurso la Presidencia de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD).

II
Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento

sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho III, de la Resolución recurrida, tal como se transcribe a continuación:

1.- PREJUDICIALIDAD PENAL.

En lo relativo a esta alegación, se quiere significar que ya ha sido contestada en la Resolución del procedimiento sancionador, de la siguiente manera:

> En relación con esta cuestión, esta Agencia considera necesario señalar que, en el presente expediente sancionador, sin embargo, 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 demanda planteada ante el órgano jurisdiccional que menciona **ORANGE**, en la medida en que el sujeto infractor no es el mismo.
>
> De este modo, **ORANGE** es el sujeto responsable en el presente procedimiento sancionador, mientras que el responsable penal sería el empleado que procedió al duplicado de la tarjeta SIM, tal y como se recoge en la demanda presentada por **ORANGE** en su escrito de alegaciones.
>
> 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 siguientes 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".*

En este punto, hay que señalar que ORANGE a lo largo de su escrito de recurso, se limita a negar la argumentación realizada en la resolución, y olvida que el objeto de este expediente es la emisión de un duplicado de tarjeta SIM a nombre de la parte reclamada, cuando no lo había solicitado, por parte de su operador **ORANGE.** Por tanto, la cuestión planteada por **ORANGE** no puede prosperar y debe ser rechazada.

2.- SOBRE EL SUPUESTO DE HECHO.

i) Sobre la consideración de la tarjeta SIM como dato personal.

Esta cuestión ha sido contestada en la resolución que ahora se recurre de la siguiente manera:

> "Con relación a esta cuestión, y como ya se incluía en el acuerdo de inicio del presente expediente sancionador, la tarjeta SIM es una tarjeta que va insertada dentro del terminal móvil. Se trata de una tarjeta inteligente, en formato físico y de reducidas dimensiones, que contiene un chip en el que se almacena la clave de servicio del suscriptor o abonado usada para identificarse ante la red, esto es, el número de línea telefónica móvil del cliente MSISDN (Mobile Station Integrated Services Digital Network -Estación Móvil de la Red Digital de Servicios Integrados-), así como el número de identificación personal del abonado IMSI (International Mobile Subscriber Identity -Identidad Internacional del Abonado móvil-) pero también puede proporcionar otro tipo de datos como la información sobre el listado telefónico o el de llamadas y mensajes.
>
> Además, la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular ya que se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador (artículo 4.1) del RGPD).
>
> Por lo tanto, la tarjeta SIM identifica un número de teléfono y este número a su vez, identifica a su titular. En este sentido la Sentencia del TJUE en el asunto C -101/2001(Lindqvist) de 6.11.2003, apartado 24, Rec. 2003 p. I-12971: «*El concepto de "datos personales" que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva "toda información sobre una persona física identificada o identificable". Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones».*
>
> En suma, tanto los datos que se tratan para emitir un duplicado de tarjeta SIM como la tarjeta SIM (Subscriber Identity Module) que identifica de forma inequívoca y unívoca al abonado en la red, son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos.
>
> En este sentido se pronuncia la Sentencia de la Audiencia Nacional de 8 de febrero de 2024, cuando afirma:
>
> "*Tenemos que partir, que la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular ya que, a tenor del artículo 4.1*

del RGPD, se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador. Pues bien, dentro del terminal móvil, va insertada la tarjeta SIM. Es una tarjeta inteligente en formato físico y de reducidas dimensiones, que contiene un chip en el que se almacena la clave de servicio del suscriptor o abonado usada para identificarse ante la red, esto es, el número de línea móvil del cliente MSISDN (Mobile Station Integrated Services Digital Network-Estación Móvil de la Red Digital de Servicios Integrados-) así como el número de identificación personal del abonado IMSI (International Mobile Subscriber Identity-Identidad Internacional del Abonado móvil-), pero también puede proporcionar otro tipo de datos como la información sobre el listado telefónico o el de llamadas y mensajes.

Y como se resalta en la resolución recurrida, desde el año 2007, en España, de conformidad con la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, se exige que los titulares de todas las tarjetas SIM, ya sean de prepago o de contrato, estén debidamente identificados y registrados. Por lo que a hora de obtener un duplicado de la tarjeta SIM, la persona que lo solicite haya de identificarse igualmente y que su identidad coincida con la del titular."

Asimismo, la Sentencia de la Audiencia Nacional de fecha 9 de febrero de 2023, también recoge lo siguiente:

"Pues bien, la tarjeta Sim es una tarjeta inteligente que se inserta dentro del terminal móvil, que contiene un chip en el que se almacena la clave del servicio de suscriptor o abonado usado para identificarse ante la red.

Así, señala la Fiscalía General del Estado, en informe de julio de 2016, citado por la resolución recurrida: "según los estándares europeos relativos a sistemas de telecomunicaciones celulares digitales, establecidos por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI), un dispositivo de comunicaciones móviles celulares plenamente operativo, denominado en lenguaje coloquial "Teléfono Móvil" se compone materialmente de dos elementos esenciales. En primer lugar, el terminal (…). En segundo lugar, el módulo de identificación de usuario, más conocido como "tarjeta SIM" (Subscriber Identity Module). Esta tarjeta SIM es intercambiable entre los diferentes terminales móviles existentes en el mercado y contiene su chip digital la información necesaria para identificar y autenticar al abonado, incluido en International Mobile Subscriber Identity (IMSI), el cual identifica de forma inequívoca al abonado en la red celular. Sin un IMSI válido los servicios de telefonía no serán accesibles, salvo en el caso de llamada de emergencia."

Por tanto, el IMSI es el código de identificación en la red de comunicaciones celulares y es fundamental para identificar al abonado, y como está almacenado en la tarjeta SIM, quien tenga dicha tarjeta (el suplantador) tiene el IMSI almacenado. Además, en cuanto el suplantador introduzca la SIM en un terminal y lo encienda, el IMSI va a ser accedido e intercambiado con la red.

Así las cosas, en la medida en que el IMSI instalado en la tarjeta SIM permite singularizar a un individuo y por tanto identificarle, ha de ser considerado como dato personal, según el artículo 4 del RGPD, que conceptúa como tal "toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

Es decir, la expedición inadecuada de la tarjeta SIM del teléfono móvil de una persona a un tercero que suplanta su identidad permite a dicho tercero acceder a la información confidencial almacenada en dicha tarjeta y a la línea del legitimo titular de la tarjeta SIM existiendo una clara pérdida de confidencialidad pues los datos son transmitidos a un tercero ilegítimamente.

Téngase en cuenta que en España desde 2007, en virtud de la Disposición Única de la Ley 25/2007, de 18 de octubre, se exige que los titulares de todas las tarjetas SIM estén debidamente identificados y registrados. Esto es importante por cuanto la identificación del abonado será imprescindible para dar de alta la tarjeta SIM, lo que conllevará que a la hora de obtener un duplicado de ésta la persona que lo solicite haya de identificarse y que su identidad coincida con la del titular.

En suma, tanto los datos personales (nombre, apellidos y DNI) que se tratan para emitir un duplicado de la tarjeta SIM, como la propia tarjeta SIM que identifica de forma inequívoca al abonado en la red, son datos de carácter personal…"

ii) Sobre la realización de operaciones bancarias.

En relación con esta alegación, hay que señalar que, a pesar de las manifestaciones de ORANGE, en las que manifiesta que esta Agencia no ha entrado a valorarlas, éstas ya han sido contestadas de la siguiente manera en la resolución del expediente sancionador:

"En este sentido, con relación al hecho de otorgar al duplicado de la tarjeta SIM la facultad de permitir la comisión de operaciones bancarias, hay que señalar que la propia **ORANGE**, al presentar la denuncia contra el agente que realizó el duplicado de la tarjeta SIM que ha motivado la apertura del presente expediente sancionador ha definido el concepto de SIM SWAPPING de la siguiente manera:

"El SIM Swapping es un ciberataque que consiste en suplantar la identidad de una persona ante su compañía de servicios telefónicos y pedir un duplicado de la tarjeta SIM de su teléfono móvil para con ello, acudir a su banca online y operar con la misma, recibiendo los SMS con el código de confirmación de operaciones bancarias en esa nueva SIM, procediendo a desviar el dinero de

la cuenta corriente de la persona suplantada hacia otra propiedad de los delincuentes.

La víctima, tal y como sucede en el presente supuesto, solo se entera de la situación cuando deja de tener cobertura en su teléfono móvil y por mucho que reinicia el dispositivo o intenta buscar cobertura no lo consigue ya que, al entrar en funcionamiento la nueva SIM duplicada que los ciberdelincuentes piden a la compañía de servicios telefónicos, la SIM que está en el teléfono de la víctima deja de funcionar."

En este sentido, la propia **ORANGE** confirma el concepto de SIM Swapping, y que tiene como objetivo poder acudir a la banca online, recibiendo los SMS con el código de confirmación de operaciones bancarias en la nueva SIM, y proceder a desviar el dinero de la cuenta corriente de la persona suplantada hacia otra de propiedad de los delincuentes. Por tanto, en este aspecto no hay ninguna duda del concepto de SIM Swapping y de las razones por las cuales se solicitan los duplicados de las tarjetas SIM.

Además, en el presente supuesto, en relación con la infracción del artículo 6 del RGPD, lo que se está analizando es la realización de un duplicado de tarjeta SIM propiedad de la parte reclamante y sin su consentimiento, en una tienda propiedad de **ORANGE**.

En cuanto a la infracción del artículo 25 del RGPD, **ORANGE** para el establecimiento de las medidas apropiadas al riesgo ha de evaluar los posibles riesgos para los derechos y libertades de las personas, entre los que se encuentra que los clientes sufran el conocido ataque SIM Swapping mediante la obtención fraudulenta de un duplicado de su tarjeta SIM, que conlleva la consiguiente pérdida de control sobre sus propios datos personales y unas posibles pérdidas financieras. Todo ello con independencia de la responsabilidad en que puedan incurrir las entidades financieras si actuaron con falta de diligencia.

Por otro lado, **ORANGE** también hace referencia a que, en el acuerdo de inicio, se hacen asociaciones erróneas para agravar el supuesto de hecho al otorgar al duplicado de la tarjeta SIM la facultad de permitir la comisión de operaciones bancarias, omitiendo el paso previo según el cual los malhechores deberán obtener y poder utilizar las credenciales bancarias de la parte reclamante para poder identificarse y realizar la suplantación de identidad ante la entidad financiera.

Añade que esta AEPD no menciona el rol que desempeñan las entidades financieras en estos supuestos, y no consta que se hayan iniciado procedimientos sancionadores contra las mismas.

Respecto de la responsabilidad de las entidades financieras, cabe señalar que la Directiva PSD2, se aplica a los servicios de pago prestados dentro de la Unión (artículo 2), y no a **ORANGE**, pero también es cierto que la expedición de un duplicado de tarjeta SIM a favor de un tercero que no es el titular de la línea, proporciona a los suplantadores el control de la línea telefónica, y por lo

tanto, de los SMS dirigidos al teléfono vinculado a la tarjeta SIM inicial y de esta manera a poder acceder a conocer el código de autentificación de la transacción.

Conforme al artículo 4.30 de la Directiva, la “autenticación reforzada” se basa en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario). Estos elementos o factores son independientes entre sí y, por tanto, la vulneración de uno no compromete la fiabilidad de los demás.

El fundamento es muy sencillo: cuantos más elementos se tengan para verificar la identidad del usuario, más segura es la transacción.

En estos casos, el suplantador, en primer lugar, deberá introducir el usuario y contraseña o password en la aplicación o en el sitio web del proveedor de servicio de pagos o de banca online. En segundo lugar, para completar la transacción o gestión electrónica que desee realizar, el suplantador recibirá, normalmente a través de un SMS, un código alfanumérico de verificación en el teléfono móvil vinculado a ese perfil. Dicho código tiene una validez temporal limitada y es de un solo uso, es decir, únicamente se genera para esa transacción concreta y durante un tiempo limitado. Una vez introducido el código de verificación, se realizaría y completaría la transacción. Se presupone que solo el usuario tiene el dispositivo móvil en su poder (sería el “algo que tiene”), por lo que al recibir en dicho teléfono móvil el código de verificación a través del SMS, su identidad quedaría doblemente autenticada. Por tanto, a los suplantadores no les bastaría para poder cometer el fraude con conocer el usuario y contraseña con los que se identifique la víctima, sino que será necesario que intercepten dicho código de confirmación. En consecuencia, para poder efectuar una transferencia, transacción o compra no consentida, es decir, para llevar a cabo la estafa informática, el ciberdelincuente deberá acceder ilegítimamente a los códigos de verificación asociados a cada una de esas operaciones remitidos por la entidad bancaria a través de SMS y la manera más habitual de hacerlo es a través de la obtención de un duplicado de la tarjeta SIM.

Por lo tanto, es necesario ejecutar dos acciones completamente diferentes pero complementarias entre sí.

En primer lugar, se han de obtener los datos de acceso a la banca online o proveedor de pago titularidad de la persona a defraudar, si nos centramos en la búsqueda del enriquecimiento patrimonial.

Y, en segundo lugar, se habrá de obtener el duplicado de la tarjeta SIM titularidad de la persona a defraudar con la finalidad de hacerse con los SMS de confirmación que el cliente recibirá en su terminal móvil como autentificación de doble factor.

Pues bien, en la última de estas acciones -obtención del duplicado-, es donde se han centrado los hechos objeto de este procedimiento y no en los

acontecidos en la primera fase, que como resulta obvio quedan al margen de la responsabilidad que se imputa a **ORANGE** en el presente procedimiento.

Por otro lado, **ORANGE** manifiesta que la AEPD pretende sancionar los fraudes SIM SWAPPING sin atender ni analizar el concreto supuesto de hecho, el perjuicio asociado, ni las responsabilidades derivadas, sin tener en cuenta la diligencia desplegada por **ORANGE** en su actuación y en la adopción de medidas de seguridad. Añade que la AEPD omite valorar la documental aportada, estableciendo un discurso genérico para legitimar una infracción a la normativa de protección de datos.

Sin embargo, en relación con esta cuestión, es necesario hacer referencia al momento procedimental en el que **ORANGE** presenta estas alegaciones. En este sentido, de conformidad con lo dispuesto en el artículo 64 de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, referido al "*Acuerdo de iniciación en los procedimientos de naturaleza sancionadora*", en el apartado 2 establece:

"*2. El acuerdo de iniciación deberá contener al menos:*

a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Identificación del instructor y, en su caso, secretario del procedimiento y norma que le atribuya tal competencia, con expresa indicación del régimen de recusación de los mismos.

d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.

e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.

f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como indicación de que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada."

Por tanto, el acuerdo de iniciación del presente procedimiento sancionador contiene todos los pronunciamientos que la normativa aplicable requiere.

Sin perjuicio de lo anterior, la alegación planteada por **ORANGE** tampoco puede ser tenida en cuenta, en la medida en que, el supuesto de hecho sí se contempla y valora a la hora de graduar la sanción asociada a las infracciones de los artículos 6 y 25 del RGPD, en el apartado a) del artículo 83 del RGPD.

En lo que se refiere a la diligencia de **ORANGE**, hay que tener en cuenta que este aspecto se ha valorado como agravante en la infracción del artículo 25 del RGPD, por lo que si se ha analizado. En relación con las medidas adoptadas con posterioridad hay que señalar que se valoran positivamente, pero no determinan que no se haya producido la infracción del artículo 25 del RGPD.

Por último, tampoco se puede tener en cuenta la afirmación realizada por **ORANGE** en relación con que esta Agencia utiliza un discurso genérico, o que no se valore la documental presentada, tal y como se puede observar en el presente documento y en el elevado número de hechos probados.

iii) Sobre la relación de los autores del hecho delictivo con ORANGE.

Esta cuestión también ha sido contestada de la siguiente manera en la resolución recurrida:

"No obstante, con relación a las manifestaciones referidas a que los agentes del encargado del tratamiento no habrían seguido las instrucciones de **ORANGE** en cuanto responsable del tratamiento, hay que tener en cuenta las Directrices 7/2020 del CEPD, que determinan que:

"30 Siguiendo la línea del enfoque basado en los hechos, la palabra «determine» significa que el ente que realmente ejerce una influencia decisiva sobre los fines y medios del tratamiento es el responsable. Por lo general, el contrato de tratamiento establece quién es la parte determinante (el responsable del tratamiento) y quién, la parte que sigue las instrucciones (el encargado del tratamiento). Incluso cuando el encargado del tratamiento ofrezca un servicio que se defina previamente de un modo concreto, deberá presentar al responsable del tratamiento una descripción detallada del servicio, y este deberá adoptar la decisión final sobre la aprobación del modo en que se efectuará el tratamiento y solicitar los cambios que considere necesarios. Además, el encargado del tratamiento no puede modificar, en un momento posterior, los elementos esenciales del tratamiento sin la aprobación del responsable.

39. La cuestión es dónde se debe trazar la línea entre las decisiones reservadas al responsable del tratamiento y aquellas que pueden dejarse a la discreción del encargado. Es evidente que las decisiones sobre el fin del tratamiento siempre deben corresponder al responsable.

40. Por lo que respecta a la determinación de los medios, cabe distinguir entre los medios esenciales y los no esenciales. Los medios esenciales se reservan tradicionalmente y de forma inherente al responsable del tratamiento. Estos deben ser determinados obligatoriamente por el responsable del tratamiento,

aunque la determinación de los medios no esenciales también puede dejarse en manos de él. Los medios esenciales son medios estrechamente ligados al fin y el alcance del tratamiento, como el tipo de datos personales tratados («¿qué datos se tratarán?»), la duración del tratamiento («¿cuánto tiempo se tratarán?»), las categorías de destinatarios («¿quién tendrá acceso a los datos?») y las categorías de interesados («¿a quién pertenecen los datos personales tratados?»). Además de estar relacionados con el fin del tratamiento, los medios esenciales se encuentran estrechamente vinculados a la cuestión de si el tratamiento es lícito, necesario y proporcionado. Los medios no esenciales están relacionados con aspectos más prácticos del tratamiento en sí, como la elección de un tipo particular de hardware o software o la decisión sobre los pormenores de las medidas de seguridad, que pueden dejarse en manos del encargado del tratamiento.

41. Pese a que las decisiones sobre los medios no esenciales pueden dejarse en manos del encargado del tratamiento, el responsable aún deberá estipular ciertos elementos en el contrato con el encargado: por ejemplo, en relación con el requisito de seguridad, podrá ordenarse la adopción de todas las medidas exigidas en virtud del artículo 32 del RGPD. El contrato también debe establecer que el encargado del tratamiento ayudará al responsable a garantizar el cumplimiento de, por ejemplo, lo dispuesto en el artículo 32. En cualquier caso, el responsable del tratamiento sigue siendo responsable de la aplicación de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento (artículo 24). Para ello, el responsable debe tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, además de los riesgos para los derechos y las libertades de las personas físicas. Por este motivo, el responsable del tratamiento debe contar con una información completa sobre los medios utilizados, ya que, así, podrá adoptar una decisión informada al respecto. Para que el responsable pueda demostrar la legalidad del tratamiento, se aconseja documentar, en el contrato u otro instrumento jurídicamente vinculante entre el responsable y el encargado, al menos las medidas técnicas y organizativas necesarias.

(…)

80. En segundo lugar, el tratamiento debe llevarse a cabo por cuenta de un responsable del tratamiento, pero no bajo su autoridad ni control directos. Actuar «por cuenta de» alguien significa servir los intereses de otro y remite al concepto jurídico de «delegación». En el caso de la normativa de protección de datos, el cometido del encargado del tratamiento es aplicar las instrucciones dadas por el responsable del tratamiento, cuando menos en lo relativo a los fines del tratamiento y a los elementos esenciales de los medios. La legitimidad del tratamiento en virtud del artículo 6 y, si procede, del artículo 9 del Reglamento deriva de la actividad del responsable, y el encargado únicamente debe tratar los datos siguiendo las instrucciones dadas por este. Aun así, tal como se ha indicado previamente, las instrucciones del responsable del tratamiento pueden dejar cierto margen de discrecionalidad sobre el modo de servir mejor a los intereses de este, de modo que permitan al encargado elegir los medios técnicos y organizativos más adecuados.32

81. Actuar «por cuenta de» alguien también significa que el encargado no puede llevar a cabo el tratamiento para sus propios fines. Tal como se estipula en el artículo 28, apartado 10, el encargado del tratamiento infringirá el RGPD cuando no se ciña a las instrucciones del responsable y comience a determinar sus propios fines y medios del tratamiento. En estos casos, el encargado del tratamiento se considerará responsable en relación con dicho tratamiento y podrá ser sancionado por no haberse adherido a las instrucciones del responsable*".*

Como ya se ha señalado anteriormente, la STJUE precitada "*un responsable del tratamiento es responsable no solo por todo tratamiento de datos personales que efectúe él mismo, sino también por los tratamientos realizados por su cuenta, puede imponerse a ese responsable una multa administrativa con arreglo al artículo 83 del RGPD en una situación en la que los datos personales son objeto de un tratamiento ilícito y en la que no es él, sino un encargado al que ha recurrido, quien ha efectuado el tratamiento por cuenta suya*".

En el presente supuesto, y tal y como se encuentra recogido en los Hechos Probados de esta Resolución, el duplicado de la tarjeta SIM se produce en un establecimiento **ORANGE** propiedad de la empresa "TOWER PHONE, S.L.," que actúa como encargada del tratamiento de **ORANGE**.

También se hace referencia al contrato de franquicia de las dos entidades, de fecha 1 de abril de 2022, en la que se podía comprobar que:

II. "(…)"

V. (…).

(…)

(…)

(…)

A todo esto, hay que añadir, como ya se ha señalado anteriormente, que el cliente, en todo momento, está contratando los servicios de telefonía con **ORANGE**, puesto que, de conformidad con todo lo señalado anteriormente y que figura en el contrato de franquicia, es **ORANGE** como responsable del tratamiento la que determina la finalidad y los medios de los tratamientos realizados para el ejercicio de la actividad, y quien realmente presta el servicio de telefonía.

Por lo tanto, en base a lo expuesto, procede desestimar esta alegación de **ORANGE**."

3.- SOBRE LA ACTUACION DELICTIVA DE LOS AGENTES.

Esta alegación fue contestada en la resolución ahora recurrida en el siguiente sentido:

> "Con esta alegación, **ORANGE** está intentado que este supuesto sea tratado de manera diferente al resto de supuestos de SIM SWAPPING, dado que el supuesto que ha motivado la apertura de este procedimiento sancionador consistiría en una variante delictiva de nuevo cuño
>
> Sin embargo, esta cuestión ya se contestó en las alegaciones al acuerdo de inicio a la que desde aquí nos remitimos, en el apartado Tercera: del rol de víctima de **ORANGE**, en el siguiente sentido:
>
> **ORANGE**, con esta alegación, pone de manifiesto que se trata de la emisión de un duplicado de tarjeta SIM realizada de manera diferente a otros supuestos, en la medida en que se había realizado por dos comerciales del punto de venta de la compañía, que actuaban, consiguientemente, en nombre de **ORANGE**.
>
> Antes de continuar con el resto de la argumentación presentada por **ORANGE**, desde esta AEPD se quiere hacer constar que la denuncia presentada ante el Juzgado de Instrucción se dirige contra ***A.A.A.***, por posible delito de:
>
> -posible delito de estafa con medios electrónicos (238.2 CP)
>
> -y/o posible delito de hurto (234 CP) y/o posible apropiación indebida (235 CP y siguientes)
>
> -y/o posible suplantación de identidad con usurpación del estado civil (401 CP)
>
> -y/o posible delito de intrusión informática e interceptación de transmisiones de datos informático (197 bis CP)
>
> - cualquier otro que se apreciara de la instrucción de la presente causa.
>
> En los hechos de la denuncia presentada se pone de manifiesto que el denunciado empezó a trabajar en el centro de trabajo ubicado en la calle ******DIRECCIÓN.1*** de Madrid, el pasado 12 de julio de 2021. El denunciado estuvo trabajando hasta el día 11 de diciembre de 2022.
>
> Además, en el Hecho cuarto de la denuncia, en el que se habla de los hechos denunciados, consta hasta 5 suplantaciones realizadas por el empleado de **ORANGE** de la calle ******DIRECCIÓN.1*** de Madrid.
>
> Por otra parte, en el Hecho tercero de la denuncia se habla del concepto de SIM SWAPPING de la siguiente manera:
>
> "*En primer lugar, es importante explicar en que consiste los hechos aquí denunciados (SIM Swapping) llevados a cabo por el denunciado* ***B.B.B.*** *en, al menos, los días 14, 17 y 21 de noviembre de 2022 en su centro de trabajo, el punto de venta ORANGE ubicado en el* ******ESTABLECIMIENTO.1*** *de Madrid* ***(***DIRECCIÓN.1***)."

Por lo tanto, aunque en sus alegaciones **ORANGE** habla de dos trabajadores de la misma tienda, se observa claramente que han sido dos trabajadores de dos tiendas diferentes los que se han podido ver involucrados en un caso como el que denunciaba la parte reclamante. Además, si tenemos en cuenta el contenido de la denuncia, en la tienda **ORANGE** ubicada en la calle ******DIRECCIÓN.1***, se vieron afectados 5 particulares, mientras que, en la tienda ubicada en el ******ESTABLECIMIENTO.1*** de Madrid, se vieron afectados (...).

Una vez hecha esta matización, en el sentido de que no eran dos trabajadores de una misma tienda los que actuaron de manera errónea, sino que se trataba de trabajadores que prestaban sus servicios en dos tiendas diferentes, y que, del contenido de la denuncia presentada por **ORANGE** ante el Juzgado de instrucción se deduce claramente que afectaron al menos a 8 personas, deben decaer las manifestaciones de **ORANGE** relativas a que no es posible exigirle la capacidad total de detección y frustración de tales actos delictivos.

En este sentido, la actuación que ha determinado que se haya producido un hecho como el que se ha denunciado viene dado por el hecho de que el procedimiento que **ORANGE** tenía implantado para realizar un duplicado de tarjeta SIM, ***(…)***

Así lo explica **ORANGE** en su escrito de alegaciones al acuerdo de inicio, de fecha 21 de diciembre de 2023, presentado ante esta Agencia, de tal manera que, según expresa **ORANGE**, "en el caso que nos ocupa, los agentes de **ORANGE** utilizaron ***(…)***, motivo por el cual, al introducirlo en el sistema de ***(…)***. Así pues, para este tipo de errores de lectura de documentación, el Protocolo de **ORANGE** establece que, si bien se debe generar un aviso al Grupo de Análisis de Riesgos, se permite a los agentes comerciales para casos tasados ***(…)***. Ello se debe a la necesaria apertura de dicha manualidad dentro de un sistema absolutamente automatizado que ha de permitir el acto comercial ***(…)***".

Es por ello que en el presente procedimiento sancionador se ha imputado la infracción del artículo 25 del RGPD, pues según reza, el responsable del tratamiento, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, debe aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

Este artículo impone una obligación de diseño de procedimientos internos en el momento de determinar los medios de tratamiento y de aplicar esos procedimientos en el momento del tratamiento, para garantizar de forma efectiva el cumplimiento de los requisitos de protección de datos.

ORANGE, al comunicar el procedimiento que tiene implantado para la expedición de duplicados de tarjeta SIM, ha informado que hay supuestos en los que se puede proceder a ***(…)***.

El principio de protección de datos desde el diseño impone que, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Con el sistema que tenía implantado **ORANGE**, según se recoge en su escrito de alegaciones al acuerdo de inicio del presente expediente sancionador, de fecha 21 de diciembre de 2023, los agentes pudieron utilizar un ***(…)*** que pueden derivarse de la entrega de una tarjeta SIM válida a un tercero sin consentimiento de su titular. Así, según aduce **ORANGE**, al introducir los agentes ***(…)***. Para este tipo de errores, según manifiestan, el Protocolo de **ORANGE** establece que, si bien se debe generar un aviso al Grupo de Análisis de Riesgos, se permite a los agentes comerciales para casos ***(…)***. Según sigue manifestando **ORANGE**, ello se debe a la necesaria apertura de dicha manualidad dentro de un sistema absolutamente automatizado que ha de permitir ***(…)***. Así las cosas, ORANGE articuló un protocolo que tenía como principal objetivo la realización del acto comercial, pero que no contemplaba el riesgo de la emisión y entrega de una tarjeta SIM a persona distinta de su titular. El aviso al Grupo de Análisis de Riesgos resulta manifiestamente ineficaz, toda vez que no logró que se detectara la suplantación, al menos, en los casos que conoce esta Agencia a través del presente procedimiento.

Por tanto, desde el diseño del tratamiento ya no existían medidas del artículo 25 del RGPD para verificar que la información introducida no era errónea, y comprobar que la solicitud de duplicado de tarjeta se estaba realizando por el titular de la línea al que, asimismo, se le realizaba la entrega.

Esto supone que **ORANGE** no habría identificado y analizado de forma adecuada los riesgos que un proceso manual de duplicados de tarjeta SIM entraña para los derechos y libertades de las personas físicas, ni previsto ni aplicado desde el diseño las medidas técnicas y organizativas apropiadas, para aplicar de forma efectiva los principios de protección de datos, que exige el artículo 25 RGPD.

El derecho fundamental a la protección de datos también incluye que los responsables del tratamiento integren la protección de datos en el diseño del tratamiento de datos personales, desde su inicio y durante todo el ciclo de tratamiento, estableciendo para ello las políticas adecuadas para el cumplimiento de este principio y la protección de los derechos de las personas, y eso es precisamente lo que no hizo **ORANGE** y lo que se está cuestionando en este procedimiento sancionador, ya que el mecanismo que tenía implantado

ORANGE no había previsto siquiera la obligación de emitir duplicados de tarjeta SIM introduciendo ***(…)***, tal y como reconoce **ORANGE** en su escrito de alegaciones.

En cualquier caso, a pesar de las manifestaciones de **ORANGE** del hecho de que los agentes se aprovecharon de sus conocimientos del sistema para cometer un acto delictivo, en su escrito de alegaciones manifiestan que "desde el 14 de diciembre de 2022, **ORANGE** ha procedido a la suspensión cautelar de la opción que permite a los agentes de punto de venta, ***(…)***." Es decir, que a pesar de todo lo manifestado y la defensa que se realiza del sistema que tenía implantado, ha decidido suspender el sistema que permite la emisión de un duplicado de tarjeta SIM utilizando ***(…)***.

ORANGE manifiesta que disponía de las medidas y procedimientos de seguridad diligente, y como consecuencia han sido los delincuentes los que han evolucionado, y que esto probaría que si disponía de un adecuado diseño de la privacidad.

Añade que la aparición de estas prácticas se habría puesto de manifiesto en el "Comité AntifraudeTeleco" celebrado en el mes de marzo de 2023, y que como consecuencia de que los Agentes sean corrompidos y puedan ejercer actividades delictivas se ha realizado una nueva evaluación del riesgo atribuido a esta amenaza, aportando una matriz de riesgo como documento nº 1, en la que se puede observar un elemento referido al SIM SWAPPING, pero que está relacionado con el Phising. Y no figura nada referido a fraude por empleados.

También figura como elemento "fraudulent Use of Data by 3rd Parties/ Payment Fraud".

ORANGE manifiesta que se puede comparar esta matriz con la aportada como documento nº 12 en las alegaciones al acuerdo de inicio. Este documento 12 se titula "2023 Non Telco Fraud Risk map. Key risk" y en él también figura un apartado referido a "Fraudulent use of Data-3rd Parties" y en este punto "***(…)"***

Sin embargo, el riesgo derivado de que los empleados puedan utilizar sus credenciales para cometer hechos delictivos no se encuentra recogido tampoco en ninguna de estas tablas. El riesgo referido a "Fraudulent use of Data-3rd parties" está redactado de manera genérica, y ello no implica que el riesgo a que hace referencia **ORANGE** se encontrara analizado y evaluado en atención a las medidas implantadas por **ORANGE**.

En este punto, **ORANGE** insiste en que no puede interpretarse que permitir a un agente de tienda tomar decisiones sobre algunas cuestiones pueda asimilarse al incumplimiento del RGPD, porque choca con la propia regulación recogida en el mismo, donde se consideraría que el riesgo reside en la adopción de decisiones automatizadas sin intervención humana. Y añadía que la finalidad de la intervención del agente era evitar que, en supuestos específicos y tasados, ***(…)*** impida al interesado el acceso a un servicio contratado.

> **ORANGE** prosigue manifestando que la Agencia categoriza la parametrización de un ***(…)*** como una vulneración del artículo 25.
>
> En relación con esta cuestión, es necesario señalar que esta cuestión también ha sido contestada en la propuesta de resolución, en el sentido de que **ORANGE** tiene implementado un sistema para la emisión de tarjetas SIM en las que ***(…)***, pero ya no solo, como manifiesta **ORANGE**, cuando el ***(…)***.
>
> ***(…)***.
>
> Así las cosas, **ORANGE** manifiesta que, ***(…)***. Tal y como señala **ORANGE** "***(…)***."
>
> Sin embargo, tal y como se ha demostrado, ***(…).***

Por todo lo expuesto, esta alegación debe ser desestimada.

4.- INEXISTENCIA DE FALTA DE LEGITIMACION EN EL TRATAMIENTO DE DATOS PERSONALES DE ORANGE.

Esta alegación de **ORANGE** ya fue contestada en la resolución ahora recurrida, del siguiente modo:

> **"ORANGE**, con esta alegación, quiere insistir en que los hechos que han motivado la apertura del expediente sancionador han sido realizados por empleados de uno de sus encargados de tratamiento, y entiende que esta Agencia pretende responsabilizar a **ORANGE** del proceder de estos agentes, sin importar que este proceder pueda constituir un ilícito penal.
>
> Esta cuestión, sin embargo, ya ha sido contestada en la alegación segunda apartado 3 del Fundamento III.
>
> Hay que recordar que lo que se está enjuiciando en este procedimiento sancionador respecto de la infracción del art. 6 del RGPD es el hecho de que se hayan tratado los datos de la parte reclamante mediante la emisión de un duplicado de su tarjeta SIM, sin que concurriera ninguna base de legitimación. Para emitir el duplicado ***(…),*** lo que demuestra que ORANGE no contaba con su consentimiento. La tarjeta SIM ha sido emitida en nombre de **ORANGE**, lo que supone que **ORANGE** sea la responsable del tratamiento y como tal la responsable de que los tratamientos que se realizan por su cuenta se basen en alguna de las circunstancias que legitiman el tratamiento de datos personales.
>
> Es **ORANGE** la que debe responder del incumplimiento en materia de protección de datos, sin perjuicio de las actuaciones posteriores que pueda llevar a cabo."
>
> Por tanto, en virtud de todo lo expuesto, procede rechazar esta alegación.

5.- DE LA CORRECTA IMPLEMENTACION DE LA PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO.

En relación con esta manifestación, hay que señalar que **ORANGE** se limita a señalar que sí cumpliría con las disposiciones del artículo 25 del RGPD. Añade que el procedimiento de duplicados de tarjeta SIM ya ha sido analizado en multitud de expedientes que han sido archivados y que en ningún momento se aludió al potencial incumplimiento del artículo 25. Para ello, hace referencia a una serie de expedientes que habrían sido archivados por parte de esta Agencia. En este sentido, llama la atención que **ORANGE** pretenda que el presente caso de SIM SWAPPING se trate de manera diferente al resto en algunas partes de su recurso, para luego hacer esta alegación basada en la doctrina de los actos propios y que, por consiguiente, en base a los expedientes archivados a la entidad, debería entenderse cumplido con las disposiciones del artículo mencionado.

Esta manifestación no puede ser tenida en cuenta, en la medida en que, por ese razonamiento, deberían archivarse todas las reclamaciones que se planteen contra **ORANGE**, y, además, a ello, hay que añadir que esos expedientes a los que hace mención no se encuentran relacionados con los supuestos SIM SWAPPING, y uno de ellos ni siquiera se refiere a **ORANGE**.

Además, hay que tener en cuenta que ORANGE reproduce casi de la misma manera las alegaciones planteadas a lo largo del procedimiento sancionador, y esta cuestión ya ha sido tratada en la resolución ahora recurrida, en la que se hacía un análisis exhaustivo de por qué no se cumplía con el artículo 25, de la siguiente manera:

> **“ORANGE** quiere manifestar que, en base a las manifestaciones recogidas en la propuesta de resolución, sí se habría tenido en cuenta la privacidad desde el diseño, en función de la documentación remitida, el diseño de protocolos y el establecimiento de medidas en aras a garantizar el cumplimiento de los principios de protección de datos.
>
> Hay que tener en cuenta que el artículo 25 del RGPD se encuadra dentro de las obligaciones generales que el Capítulo IV del RGPD establece al responsable del tratamiento, imponiendo una obligación de diseño en el momento de determinar los medios de tratamiento, los cuales deben garantizar de forma efectiva el cumplimiento de los principios de protección de datos.
>
> El RGPD exige a los responsables establecer las medidas técnicas y organizativas necesarias a lo largo de todo el ciclo de vida del tratamiento, tanto desde el momento inicial en que se lleva a cabo la definición del tratamiento y se determinan los medios como durante su puesta en marcha y funcionamiento habitual.
>
> La protección de datos desde el diseño tiene por objetivo aplicar los principios de protección de datos en los procesos de diseño de los sistemas y procedimientos de la organización sobre los que se apoya el tratamiento de los datos, con un fin eminentemente preventivo y orientado tanto a evitar posibles

daños a las personas físicas como, de manera colateral, los perjuicios que para la organización podría suponer la modificación o el rediseño de los sistemas en los que se llevan a cabo los tratamientos, una vez desarrollados e implantados, como consecuencia de la identificación de errores de diseño que pudieran suponer daños o perjuicios a los interesados y a sus derechos y libertades.

En este orden de ideas, el considerando 78 del RGPD dispone:

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

En concreto, a la luz del considerando 78 del RGPD, el principio de protección de datos desde el diseño es la clave a seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

El principio de privacidad desde el diseño es una muestra del paso de la reactividad a la proactividad y manifestación directa del enfoque de riesgos que impone el RGPD. Parte de la responsabilidad proactiva, impone que, desde los estadios más iniciales de planificación de un tratamiento debe ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Así, y respecto de los riesgos que pueden estar presentes en el tratamiento, el responsable del tratamiento llevará a cabo un ejercicio de análisis y detección

de los riesgos durante todo el ciclo de tratamiento de los datos, con la finalidad primera y última de proteger los derechos y libertades de los interesados, y no sólo cuando efectivamente se produce el tratamiento. Así se expresa en las Directrices 4/2019 del CEPD relativas al artículo 25 Protección de datos desde el diseño y por defecto adoptadas el 20 de octubre de 2020.

En las citadas Directrices se indica al respecto que:

"35. El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del software y hardware y los servicios de tratamiento de datos.

36. Tomar en consideración la PDDD desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas"

Asimismo, las citadas Directrices 4/2019 del CEPD disponen que "*61. Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD*".

La Guía de Privacidad desde el Diseño de la AEPD afirma que "*La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada*".

La Guía dispone que "*La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña (…) La privacidad nace en el diseño, antes de que el sistema esté en*

funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida de los datos".

Por tanto, las medidas a las que hace referencia el artículo 25 del RGPD pretenden que la empresa tenga integrada dentro de la misma la protección de datos de carácter personal, incluso antes de iniciarse materialmente el tratamiento de los datos personales.

De esta forma, se apuesta porque la protección de datos de carácter personal sea tenida en consideración desde un primer momento, desde la toma de decisiones o del momento de la planificación.

ORANGE, en su escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, pone de manifiesto que cumple con las previsiones del artículo 25. Para ello, ha manifestado que es la oficina del Delegado de Protección de Datos de la compañía quien interviene para permitir el lanzamiento de proyectos, productos y servicios que puedan impactar en el tratamiento de datos personales de los clientes y usuarios de **ORANGE**, y así vendría recogido en los siguientes documentos, que aporta junto a su escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador:

- Documento 5 relativo al "Privacy Management Dashboard", que, según manifiesta **ORANGE**, anualmente se comparte con la compañía.

Este documento que aporta **ORANGE** es un formulario en inglés, referido al año 2023, y en el que hay que ir completando campos relativos al tratamiento de datos personales que se procesen en la compañía.

-Documento 6, que es un informe que contiene la opinión de la auditoría correspondiente a la aplicación de los principios de privacidad desde el diseño y por defecto. Es un informe en que el que se extraen unas conclusiones en las que no se concreta ningún tipo de actuación, sino que desde **ORANGE** se tiene en cuenta "*la aplicación del Principio de PbDg con el objeto de intentar anticiparse de forma proactiva a los eventos que puedan afectar a la privacidad evitando, en la medida de lo posible, su materialización y, por tanto, el impacto sobre los derechos y libertades de los afectados en materia de protección de datos*."

-Documento 7, que viene titulado como el "Procedimiento de Protección de Datos desde el diseño y por defecto". En este documento se observa que se pretende la aplicación de este principio, pero no viene materializado en procesos concretos, sino que únicamente se manifiesta que será tenido en cuenta.

De esta documentación se concluye que, en estos documentos se hace una referencia genérica a la posibilidad de la existencia de riesgos, pero no se identifican de manera concreta, y no se prevén actuaciones en concreto con respecto a la posibilidad de que se produzcan. No se trata de documentos de los que, tras una evaluación de los riesgos que implica la entrega de un duplicado de la tarjeta SIM a un tercero no autorizado, se derive la aplicación

de unos determinados procedimientos, desde el inicio del tratamiento, que contemplen medidas concretas eficaces para su mitigación.

No se debe olvidar que el RGPD pretende lograr la protección de los derechos de los interesados, y, por lo tanto, el foco debe dirigirse a la identificación y evaluación de los riesgos en los derechos y libertades de los interesados, con la posterior adopción de las medidas técnicas y organizativas de todo tipo destinadas a evitar su materialización.

De este modo, si el enfoque de la empresa no está orientado a los riesgos para los derechos y libertades de los interesados, como ocurre en el presente caso, no solo no se va a procurar una protección eficaz a los interesados, sino que supone un incumplimiento del artículo 25 del RGPD.

En sus alegaciones al acuerdo de inicio del presente procedimiento sancionador, **ORANGE** manifiesta que la actuación que ha motivado la apertura de este procedimiento sancionador viene motivada por la actuación dolosa de un agente que ha provocado un error en el sistema para permitir la realización de un acto comercial haciendo un mal uso de sus permisos. Añade **ORANGE** que este fraude estaba considerado como de bajo riesgo.

También pone de manifiesto que, a la hora de explicar que este proceso que, "*no debe perderse en ningún momento de vista que ORANGE es una empresa de telecomunicaciones que da servicios a sus clientes, y que estos demandan agilidad en la realización de los tramites y gestiones que solicitan. La demora en estas gestiones es percibida de forma negativa, lo que obliga a que los protocolos establecidos sean compatibles con una experiencia de usuario adecuada y, por tanto, disponer de diferentes opciones para atender las necesidades de los clientes*."

Con esta afirmación se está primando la celeridad en el proceso de atención a los clientes a las garantías de los derechos de los particulares.

ORANGE también ha manifestado que la implementación y supervisión de las medidas de seguridad técnica está encomendada al departamento de sistemas, en el caso de la detección del fraude, aunque la detección de su posibilidad venga identificada por la oficina del DPO o cualquier otra área, mientras que la gestión está coordinada desde el departamento específico de la compañía especializado en la prevención del fraude, que es quien evalúa los riesgos conforme a un protocolo y metodología específica, aportando para acreditarlo los siguientes documentos, que son:

1. Documento 8, relativo a la "group RIsk Management Policy".

Este documento es un documento aportado en inglés, en el que se hace referencia de manera teórica a lo que se considera un riesgo

2. Documento 9 que contiene la Política de Control y Gestión de Riesgos.

Este documento está redactado en español y en la introducción se recoge que es un modelo de Control y Gestión de Riesgos de **ORANGE** España, que se enmarca dentro de la metodología desarrollada por el grupo **ORANGE**, pero el documento está redactado de manera teórica, de tal manera que no se hace mención alguna de forma concreta a la posibilidad de que un empleado pudiera ***(…)***.

3. Documento 10 que describe el funcionamiento del Comité de Riesgos Locales

4. Documento 11 que enumera la Política de Control Interno de **ORANGE**.

De estos documentos se concluye que se trata de una documentación en la que se hace referencia a la posibilidad de la existencia de riesgos, pero no se identifican de manera concreta, y no se prevén actuaciones en concreto con respecto a la posibilidad de que se produzcan situaciones como las que se han producido en el presente expediente sancionador, en la medida en que no se hace mención alguna de forma concreta a la posibilidad de que un empleado pudiera ***(…)***.

No se debe olvidar que el RGPD pretende lograr la protección de los derechos de los interesados, y, por lo tanto, el foco debe dirigirse a la identificación y evaluación de los riesgos en los derechos y libertades de los interesados, con la posterior adopción de las medidas técnicas y organizativas de todo tipo destinadas a evitar su materialización.

De este modo, si el enfoque de la empresa no está orientado a los riesgos para los derechos y libertades de los interesados, sino que está dirigido a los riesgos para la propia empresa, no solo no se va a procurar una protección eficaz a los interesados, sino que supone un incumplimiento del artículo 25 del RGPD.

ORANGE también ha manifestado su disconformidad con el hecho de que en los procesos no pueda llevarse a cabo una intervención humana. Sin embargo, en este punto, lo que se está cuestionando es que **ORANGE** no tenía previsto ningún control para casos en que se pudiera ***(…)***.

De este modo, la contestación que ha dado **ORANGE** no puede ser estimada puesto que no se está exigiendo un proceso totalmente automatizado, sino que en la implantación del sistema no se previó el riesgo, al no tener implantado ningún mecanismo para evitar un uso incorrecto de sus protocolos manuales. Todo ello, si tenemos en cuenta que el procedimiento habitual para la emisión de duplicados de tarjeta SIM de **ORANGE** es automatizado, y ha manifestado en este mismo escrito de alegaciones que ha suspendido la posibilidad de validación manual de los documentos de identidad de los solicitantes de tarjeta SIM.

Además, como ya se ha señalado anteriormente, no se puede olvidar tampoco que **ORANGE** ha manifestado, a la hora de explicar este proceso que, "*no debe perderse en ningún momento de vista que ORANGE es una empresa de telecomunicaciones que da servicios a sus clientes, y que estos demandan*

agilidad en la realización de los tramites y gestiones que solicitan. La demora en estas gestiones es percibida de forma negativa, lo que obliga a que los protocolos establecidos sean compatibles con una experiencia de usuario adecuada y, por tanto, disponer de diferentes opciones para atender las necesidades de los clientes."

Por todo lo expuesto no puede ser tenida en cuenta esta alegación de **ORANGE**, en la medida en que no se trata de no poder automatizar los procedimientos, sino que se trata de que la agilidad en las gestiones no justifica ni puede ser impedimento para no cumplir con lo previsto en la normativa de protección de datos, de obligatorio cumplimiento en aquellos casos, como el presente, en que se están tratando datos de carácter personal de los interesados.

En este sentido, el proceso para la emisión de duplicados de tarjeta SIM lleva aparejados unos controles y medidas de seguridad destinadas a garantizar que las SIM sean emitidas a solicitud de los clientes y una vez verificada su identidad, habiéndose tenido en cuenta la protección de la privacidad de los interesados, y cree que esta Agencia trata de descalificar la prueba documental bajo la única premisa de que se ha producido un supuesto concreto en la que ha mediado un delito.

Añade que **ORANGE** sí dispone de políticas encaminadas a garantizar la aplicación de los principios de protección de datos en sus procesos de negocio, independientemente de que no se identifique en cada uno de ellos la referencia específica a las garantías en materia de privacidad, ya que, si bien abordan los riesgos asociados en esta materia, no es la única que se tiene en cuenta, del mismo modo que no se especifican en cada uno de ellos los riesgos penales analizados, o los riesgos económicos o los reputacionales.

En este sentido, como ya se recogía en la propuesta de resolución, el principio de protección de datos desde el diseño impone que, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Por tanto, desde el diseño del tratamiento ya no existían medidas del artículo 25 del RGPD ***(…)***. La ausencia de medidas para garantizar que la solicitud de duplicado de tarjeta se realizaba por el titular de la línea, unido a que tampoco se comprobaba que se realizaba la entrega al titular, es lo que constituye un incumplimiento del principio de protección de datos desde el diseño.

Esto supone que **ORANGE** no habría identificado y analizado de forma adecuada los riesgos que ***(…)***, ni previsto ni aplicado desde el diseño las medidas técnicas y organizativas apropiadas, para aplicar de forma efectiva los principios de protección de datos, que exige el artículo 25 RGPD.

ORANGE se limita a decir que cumplía con los requisitos previstos, y aporta una documentación en la que se dice que tiene en cuenta este artículo, pero en ninguna de ellas se indica precisamente que se había implementado el principio de protección de datos desde el diseño y por ***(…)***.

Para solventar esta cuestión, manifiesta que la documentación inicial que ya ha proporcionado es la información inicial que se facilita para cualquier proyecto en el que se traten datos personales en aras a comenzar a regular las distintas actividades desde una perspectiva que vele por la privacidad y la protección de datos personales, y que, para cada caso particular se aplican las medidas que se consideran correspondientes, como puede ser la formación de personal encargado de los procesos. Sin embargo, sigue sin presentar dicha documentación. Manifiesta que aportó el documento nº 12, en las alegaciones al acuerdo de inicio, que junto con el documento 1 presentado en el escrito de alegaciones a la propuesta de resolución, acreditarían que sí se tenía identificado el riesgo.

Sin embargo, desde esta Agencia se entiende que dichos documentos no acreditan el cumplimiento del principio de protección de datos desde el diseño. El citado documento nº 12 a que hace referencia está fechado en el año 2023 y se titula ***(…).***

En el documento denominado 1 de las alegaciones a la propuesta de resolución, se aporta una matriz de riesgos en la que se identifica el riesgo “Fraudulent use of data-3rd parties”, sin más desarrollo y se evalúa como riesgo bajo pero no se indica si el riesgo es para los derechos y libertades de los interesados o para la continuidad en el negocio.

ORANGE aporta como documento 2 de sus alegaciones a la propuesta el acta del comité de Riesgos Local del año 2022 en la que se aprueba la política de gestión de riesgos OSP y la matriz de riesgo OSP, entre otras cuestiones, pero de su contenido parece desprenderse que en ellas se evalúa el riesgo para la continuidad del negocio.

También aporta el documento nº 3 el mapa de riesgos residuales desde la óptica de los derechos y libertades de los interesados referido al año 2022 donde se identificaba al riesgo de fraude como bajo, y que según ORANGE fue tratado en el Comité de riesgos Local del año 2022 cuya acta se adjuntaba como documento nº 2.

En este sentido, la citada acta del Comité de Riesgos Local, de fecha 3/10/2022 recoge en el apartado 6. Riesgos: Integración Mapas de riesgos:

“(…).”

A su vez, en el apartado 8 del acta: Fraude Telco se recoge:

“***(…)***.”

En el apartado 9 referido a Fraude non Telco se añade:

"(…)."

En cuanto al mapa de riesgos aportado como documento nº 3, titulado 2022 Non Telco Fraud risk map: Fraudulent use of Data-3rd parties contiene ***"(…)"***

Y recoge lo siguiente:

"(…)".

Pues bien, según las alegaciones de **ORANGE** este documento se habría presentado al Comité cuya acta ha aportado como documento nº 2, y se habría tratado en el mismo, y sin embargo no hay ninguna referencia al mismo en la referida acta del comité.

Además, hay que tener en cuenta que, a pesar de las manifestaciones de **ORANGE**, desde esta Agencia se sigue manteniendo que no se han previsto los riesgos para los derechos y libertades derivados ***(…)***. No se ha tenido en cuenta el riesgo interno de que los empleados puedan cometer algún tipo de infracción, pero es que además se entiende que el impacto no puede ser calificado como limitado basado en que las entidades bancarias deban devolver cualquier cargo realizado por conculcación de sus sistemas.

A la vista está este supuesto en el que la parte reclamante había sufrido pérdidas económicas que ascienden a 9.000 euros, sin olvidar que en la denuncia ante el Juzgado que **ORANGE** ha presentado en su escrito de alegaciones al acuerdo de inicio, son más las personas las que se podrían haber visto afectadas, aunque no hayan presentado reclamación en la AEPD. De este modo, el impacto que este riesgo tiene en los derechos y libertades de las personas es elevado, por ello el riesgo residual no puede ser calificado como bajo sin la implantación de medidas adecuadas.

Por todo ello, desde esta Agencia se ha considerado que, a pesar de haber presentado un documento que tendría como fecha 2022, se entiende que con ello no se puede determinar el cumplimiento del artículo 25 del RGPD.

ORANGE, en su escrito de recurso, "insta a esta Agencia a que enumere qué medidas son las adecuadas para este tipo de circunstancias en las que, un empleado de un encargado del tratamiento (una distribuidora), bajo su criterio y en base a un análisis de riesgo, considera oportuno emitir un duplicado de tarjeta SIM cometiendo un delito, aun a sabiendas de que existe trazabilidad para determinar quien lleva a cabo dicha actuación". Desde esta Agencia se quiere manifestar que es **ORANGE** quien conoce a su organización, y es ella la que debe tener en cuenta las medidas a implementar, no procediendo ningún pronunciamiento al respecto.

Además, aporta dos informes periciales en los que, desde la perspectiva de la seguridad y de la analítica de procesos, pretende acreditar que **ORANGE** aplica, tanto en el momento de determinar los medios, como en el momento del propio tratamiento, que sí tiene medidas técnicas y organizativas apropiadas acordes a los riesgos

identificados, concebidas para cumplir con los requisitos del artículo 25 del RGPD y proteger los derechos de los interesados.

A pesar de las manifestaciones de **ORANGE**, con estos documentos nuevos aportados en fase de recurso se evidencia aún más lo que ya se ha recogido en la resolución ahora recurrida, y es que no tenía analizados los riesgos que para las personas físicas podía producir un caso como el que nos ocupa.
Estos informes están elaborados teniendo en cuenta siempre a la organización que los ha encargado y no tiene en cuenta los riesgos que pueden producir en los derechos y libertades de las personas físicas.

Es por ello, que se desestima esta alegación.

6.- SOBRE LA EXISTENCIA DE UN CONCURSO DE INFRACCIONES.

Esta alegación ya ha sido contestada en la resolución ahora recurrida del siguiente modo:

> "**ORANGE** entiende que en el acuerdo de inicio se hace referencia a un único hecho, sujeto y fundamento, que sería la adopción de medidas en el procedimiento de duplicado de la tarjeta SIM en los supuestos tasados de intervención manual, lo que constituiría un supuesto de concurso medial en la vía penal o una concurrencia de ofensas o delitos en vía administrativa, que aplica "siempre que la aplicación de una disposición impida o subsuma la aplicabilidad de la otra", y que hace que resulte contrario al ordenamiento jurídico sancionar dos veces al infractor por el mismo ilícito.
>
> **ORANGE** entiende que, del acuerdo de inicio se extrae que, en relación con los hechos analizados, existe una conexión directa entre las vulneraciones de los dos artículos.
>
> De esta manera, la infracción del artículo 6.1 RGPD, o la existencia de un supuesto tratamiento de datos ilícito fue necesaria e inevitable para que tuviera lugar una vulneración del principio de privacidad desde el diseño y por defecto, derivada de no existir medidas de seguridad suficientes. De este modo, si **ORANGE** hubiera tenido medidas que permitiesen evitar el duplicado de la tarjeta SIM no se habría podido concluir la infracción del principio de privacidad por diseño y por defecto del artículo 25 del RGPD.
>
> En consecuencia, se estaría dando un concurso de infracciones, ya que la comisión de una implicaría necesariamente la comisión de la otra.
>
> No obstante, en relación con esta cuestión, hay que tener en cuenta que los artículos 6.1 y 25 se encuentran tipificados de manera diferenciada en el RGPD, se califican de manera diferenciada a efectos de prescripción por la LOPDGDD y cada uno de ellos goza de entidad propia.
>
> Si la afirmación de **ORANGE** fuera cierta, no se tipificarían las infracciones a dichos artículos como infracciones diferentes.

De este modo, el artículo 6.1 del RGPD, establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

En el presente supuesto, se imputaba a **ORANGE** la emisión de una tarjeta SIM a nombre de la parte reclamante, sin que ésta la hubiera solicitado y su entrega a un tercero no autorizado.

ORANGE así lo ha reconocido, tanto en su escrito de fecha 30 de enero de 2023, como en su escrito de fecha 30 de marzo de 2023, afirmando que dicho duplicado se habría producido, el día 15 de noviembre de 2022, sin que éste hubiera sido solicitado por la parte reclamante.

Por tanto, **ORANGE** expidió una tarjeta SIM a un tercero que no era el titular de la línea, y sin seguir el procedimiento implantado por ella misma, puesto que el duplicado de la tarjeta se ha expedido sin que hubiera sido solicitado por ***(…)*** de la línea. En definitiva, realizó estas operaciones de tratamiento de datos personales sin que concurriera ninguna de las bases de legitimación que contempla el art. 6 del RGPD.

En consecuencia, ha quedado en entredicho la diligencia empleada por **ORANGE** en la identificación de la persona que solicita el duplicado.

En ese sentido el Considerando 40 del RGPD señala:

"(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."

Por otro lado, con carácter general, **ORANGE** trata los datos de sus clientes al amparo de lo previsto en el artículo 6.1.b) del RGPD, cuando se considera un tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. Para el resto de los casos, la licitud del tratamiento se fundamenta en las bases previstas en el artículo 6.1.a) c), e) y f) del RGPD.

Como ya se ha señalado anteriormente, el tratamiento realizado por **ORANGE**, en este caso, no se puede basar en lo previsto en el apartado b del artículo 6.1, ya que este duplicado de tarjeta SIM no se basaba en la ejecución de ningún contrato, al no ser necesario para su ejecución ni haber sido solicitado por la parte reclamante, tampoco el tratamiento se basaba en alguna otra de las previstas en el artículo 6.

Por otro lado, el artículo 25 del RGPD dispone:

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

2.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

Como puede observarse, dicho artículo parte de la necesidad de tener en cuenta una serie de elementos:

-Estado de la técnica
-Coste de la aplicación
-Naturaleza, ámbito, contexto y fines del tratamiento
-Riesgos que entraña el tratamiento para los derechos y libertades de las personas físicas.

Además, impone una obligación al responsable, que es quien determina los fines y los medios del tratamiento, dándose especial relevancia a los medios.

Y debe aplicar, tanto al determinar los medios del tratamiento, como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías que sean necesarias en el tratamiento.

Con ello, se persigue un doble fin:

-cumplir los requisitos del RGPD
-proteger los derechos de los interesados.

En este punto, también es necesario tener en cuenta lo dispuesto en el considerando 78 del RGPD anteriormente reproducido.

De este modo, las medidas que prevé el artículo 25 del RGPD no son medidas de seguridad exclusivamente, sino que se pretende que la empresa u organización tenga integrada dentro de la misma, de su organización, de su funcionamiento ordinario, la protección de datos de carácter personal desde el diseño. Es decir, que sea parte integrante y relevante dentro de la misma, antes incluso de iniciarse materialmente el tratamiento de datos personales, desde la toma de decisiones o del momento de la planificación.

La obligación afecta a toda la organización e implica un proceso continuo de revisión y retroalimentación con el fin de verificar si todas las medidas técnicas y organizativas existentes, de todo tipo e implementadas por la organización resultan adecuadas con el fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados. De esta forma, en caso de no resultar adecuadas, podrían ser modificadas, o en su caso, reforzadas, incorporando nuevas medidas que garanticen una más adecuada protección de los datos de carácter personal.

Por lo tanto, de conformidad con todo ello, se puede apreciar que la perspectiva o el ángulo a través del cual se contempla la realidad es diferente a lo previsto en el artículo 6 del RGPD.

En este sentido, el RGPD articula un sistema completo destinado a garantizar la protección de los datos de carácter personal de los ciudadanos, y para ello, va centrando su atención en distintos aspectos que deben ser examinados por los responsables o encargados del tratamiento.

Cada artículo constituye un ángulo desde el que observar la realidad con el fin de articular las medidas que garanticen una adecuada protección de los datos de carácter personal, y que deben ser tenidos en cuenta para articular una protección acorde con lo dispuesto en el RGPD.

En su escrito de alegaciones al acuerdo de inicio **ORANGE** pone de manifiesto que "*la infracción del artículo 6.1 RGPD, o la existencia de un supuesto tratamiento de datos ilícito fue necesaria e inevitable para que tuviera lugar una vulneración del principio de privacidad desde el diseño y por defecto, derivada de no existir medidas de seguridad suficientes. De este modo, si ORANGE hubiera tenido medidas que permitiesen evitar el duplicado de la tarjeta SIM no se habría podido concluir la infracción del principio de privacidad por diseño y por defecto del artículo 25 del RGPD*".

Sin embargo, esta manifestación no puede ser acogida, pues como se ha indicado se trata de infracciones que requieren para su comisión la concurrencia de distintos elementos, así, por un lado, resulta necesario para la comisión de la infracción del artículo 6 del RGPD, la realización de un tratamiento de datos personales sin haber comprobado diligentemente que concurría una base de legitimación para ello. Y por otro, la infracción del artículo 25 requiere la falta o deficiente implantación desde el diseño de medidas apropiadas para cumplir con el RGPD, lo que puede suceder independientemente de que se produzca un tratamiento de datos sin base de

legitimación. Obviamente en ambas infracciones ha de concurrir falta de diligencia, pero respecto de conductas diferentes.

ORANGE cita la Sentencia de la Audiencia Nacional de 24 de abril de 2013, Rec. 69/2011 según la cual:

""*Para enjuiciar esta según infracción deviene esencial, a juicio de la Sala, hacer referencia al concurso de infracciones cuya existencia se invoca igualmente en la demanda. A tal fin ha de traerse a colación lo dispuesto en el artículo 4.4 del Real Decreto 1398/1993, según el cual: en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida.*

Precepto que ha sido interpretado por la STS de 8 de febrero de 1999 (Rec. 9/1996) en el sentido de que la aplicación del concurso medial exige una necesaria derivación de unas infracciones respecto de las demás y viceversa, por lo que es indispensable que las unas no puedan cometerse sin ejecutar las otras"

Entiende **ORANGE** que, en caso de apreciarse una infracción de los artículos 6.1 y 25 del RGPD se trataría de infracciones concurrentes, y que la sanción aplicable sería en todo caso la correspondiente al incumplimiento del artículo 6.1 RGPD, teniendo en cuenta lo dispuesto en el artículo 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, según el cual:

"*cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*."

No obstante, hay que tener en cuenta, además de lo anteriormente manifestado por esta Agencia, que, en primer lugar, el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD.

1. El RGPD es un sistema completo.

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

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

contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

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

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

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

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

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

Sigue indicando el considerando 13 del RGPD que,

"(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados

con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". (el subrayado es nuestro)

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

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

De esta forma las medidas correctivas, que son todas las previstas en el art. 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.
Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

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

Las multas han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

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

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

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

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

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

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

En el supuesto concreto examinado, y sin perjuicio de lo antedicho, se debe destacar que no hay concurso medial.

El artículo 29.5 de la LRJSP establece que *“Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*”.

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

Los hechos constados determinan, como se ha dicho, la comisión de dos infracciones distintas, sin que la conculcación del artículo 6 del RGPD (falta de legitimación en la emisión del duplicado de la tarjeta SIM de la parte reclamante), tal y como asevera **ORANGE**, sea el medio necesario por el que se produce la infracción del artículo 25 del RGPD.

Por último, **ORANGE** hace referencia a las Directrices 4/2022 sobre el cálculo de multas administrativas bajo el RGPD, donde se estipulan los criterios que debe seguir la autoridad administrativa para evaluar, de forma previa a la imposición de la sanción, la posible concurrencia de éstas.

En relación con la cita de las Directrices 04/2022 del CEPD sobre el cálculo de multas administrativas conforme al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, en su apartado 22 se hace referencia a tres tipos de concurrencias, a saber, de infracción, unidad de acción y pluralidad de acciones:

“Al examinar el análisis de las tradiciones de los Estados miembros en materia de normas de concurrencia, tal como se indica en la jurisprudencia del TJUE5, y teniendo en cuenta los diferentes ámbitos de aplicación y las consecuencias jurídicas, estos principios pueden agruparse aproximadamente en las tres categorías siguientes: - Concurrencia de infracciones (capítulo 3.1.1), - Unidad de acción (capítulo 3.1.2), - Pluralidad de acciones (capítulo 3.2).

En los supuestos de concurrencia de infracciones la previsión establecida al respecto es la contenida en el artículo 83.3 del RGPD que establece un límite cuantitativo en estos supuestos de concurrencia:

“*Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves*.” (el subrayado es nuestro).

Si admitiéramos el argumento esgrimido por **ORANGE** podría extraerse que la “plena aplicabilidad del concurso medial” referido a la aplicación preferente del artículo 29 de la LRJSP, en su única pretensión de pagar una única multa en lugar de las dos impuestas, desplazan o anulan la vigencia del artículo 83.3 del RGPD, por lo que resulta contrario al ordenamiento jurídico.

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

Por último, no es cierto que el incumplimiento del artículo 25 del RGPD requiera un tratamiento de datos sin base de legitimación. El artículo 25 impone una obligación al responsable de adoptar las medidas necesarias para cumplir con el principio de protección de datos desde el diseño, sin que sea necesario que la falta de medidas o su deficiente implantación ocasione cualquier otro resultado contrario al RGPD. Es el incumplimiento de lo dispuesto en el artículo 25 lo que se sanciona, lo que puede suceder independientemente de que se produzca un tratamiento de datos sin base de legitimación, por lo que procede rechazar dicha alegación.”

Por todo lo expuesto, se desestima la presente alegación.

7.- SOBRE LA INADMISIBILIDAD DE LA RESPONSABILIDAD OBJETIVA.

Esta alegación ya fue contestada en la resolución ahora recurrida del siguiente modo:

“En relación con esta cuestión, **ORANGE** pone de manifiesto que el acuerdo de inicio del presente expediente sancionador se basa en un análisis de resultado, en la medida en que consideraría que la emisión del duplicado de la tarjeta SIM conlleva automáticamente la consideración de que no se tomaron medidas

adecuadas, surgiendo así automáticamente la responsabilidad directa por parte de **ORANGE**, estableciéndose una obligación de resultado.

ORANGE añade que esta AEPD limita la obligación al resultado, al señalar que la superación de las medidas por los agentes de **ORANGE** conlleva la consideración automática de que las medidas eran insuficientes, y que este hecho supone adoptar un principio de responsabilidad objetiva vetado por nuestro ordenamiento jurídico en numerosas ocasiones por el Tribunal Constitucional.

Contrariamente, esta Agencia considera que se han puesto de manifiesto las deficiencias observadas en las medidas desde el diseño adoptadas por **ORANGE** que evidencian el incumplimiento del art. 25 del RGPD.

En el presente procedimiento se está analizando el riesgo existente que se produce a partir de la aplicación llamada PSD2, que es cuando se empieza a realizar el tipo de fraude detallado en el presente expediente sancionador, mediante la utilización de un duplicado de tarjeta SIM obtenido indebidamente por persona distinta a su titular.

Así, la infracción devino no solo por la carencia de unas medidas para la expedición de los duplicados SIM, sino por la necesidad de su revisión y refuerzo. Así se determina en el artículo 25 del RGPD cuando establece: "…*el responsable del tratamiento aplicará, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas*…"

No basta con implantar unas medidas técnicas y organizativas, sino que hay que adecuarlas y revisarlas para mitigar los riesgos. El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados, como ocurre con el ataque SIM swapping, utilizado desde hace tiempo por los ciberdelincuentes para llevar a cabo la estafa informática. No se trata de una operativa desconocida para **ORANGE** cuyo uso haya podido sorprenderla, por lo que al evaluar los riesgos debió tener en cuenta éste, que se traduce en una mayor utilización por los delincuentes de mecanismos para apoderarse del duplicado de las tarjetas SIM de los clientes, lo que no puede ser ignorado por **ORANGE**. En este contexto, el RGPD exige que los responsables del tratamiento revisen las medidas desde el diseño, estableciendo las adecuadas para demostrar que se garantizan los derechos y libertades de las personas, teniendo en cuenta entre otros, los "riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (artículo 24.1) aplicando las medidas oportunas.

En el presente supuesto, las medidas técnicas y organizativas implementadas desde el diseño no han resultado eficaces, tal y como se ha constatado en el presente procedimiento sancionador.

Las medidas técnicas y organizativas deben garantizar un nivel de protección adecuado al riesgo, lo que en este caso no se ha hecho.

Para seleccionar las medidas adecuadas, el responsable debe basarse en los riesgos para las personas físicas, así como en lo que es razonable y técnicamente posible. El artículo 28.2.a) de LOPDGDD establece algunos supuestos en los que ya avisa que es necesario tratar mayores riesgos que los que el responsable pudiera estimar si sólo tuviera en cuenta sus propios intereses (usurpación de identidad, perjuicios económicos…).

Como ya se ha señalado anteriormente en este procedimiento sancionador, la tarjeta SIM constituye el soporte físico a través del cual se accede a los datos de carácter personal de la persona afectada. Si no se garantiza su disposición y control, el acceso a los datos personales del titular, así como el uso o usos posibles por terceros, se convierte en una amenaza que puede tener efectos devastadores en la vida de estas personas.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

El enfoque de riesgos y el modelo flexible al riesgo impuesto por el RGPD -partiendo de la doble configuración de la seguridad como un principio relativo al tratamiento y una obligación para el responsable o el encargado del tratamiento- no impone en ningún caso la infalibilidad de las medidas, sino su adecuación constante a un riesgo, que, como en el supuesto examinado es cierto, probable y no desdeñable, alto y con un impacto muy significativo en los derechos y libertades de los ciudadanos.

En la instrucción del procedimiento se ha constatado que no se habían adaptado las medidas técnicas y organizativas desde el diseño a los riesgos que supone la evolución tecnológica, lo que pone en grave riesgo los derechos de los interesados, pues las medidas no eran eficaces para evitar o mitigar el mayor riesgo de fraude que podía generarse en la solicitud de duplicados de tarjetas SIM, con la finalidad de perpetrar un ataque de SIM *swapping.*

Además, **ORANGE** no puede negar el hecho de que trata datos de carácter personal a gran escala. De este modo, efectivamente, en materia sancionadora rige el principio de culpabilidad (STC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa. Como dice la STS de 23 de enero de 1998 , *"...puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril , al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho"*.

La falta de diligencia a la hora de implementar en origen las medidas adecuadas para comprobar que la persona que solicita o activa el duplicado de una tarjeta SIM es el titular de esta es, precisamente, lo que constituye el elemento de la culpabilidad.

En cuanto a que **ORANGE** fue víctima de fraude, cabe señalar, además, que **ORANGE** debe estar en disposición de establecer mecanismos que impidan que se produzca la duplicación fraudulenta de las tarjetas SIM, medidas que respeten la integridad y confidencialidad de los datos y que impidan que un tercero acceda a datos que no son de su titularidad, pues precisamente compete a la operadora tratar datos de carácter personal conforme al RGPD (considerandos 76, 77, 78, 79, 81 y 83 RGPD; artículo 32 del RGPD y artículo 28 de la LOPDGDD).

Las pruebas periódicas, la medición y la evaluación de la efectividad de las medidas técnicas y organizativas aplicadas al tratamiento son responsabilidad de cada responsable y encargado del tratamiento conforme al RGPD.

Por lo tanto, **ORANGE** como responsable del tratamiento está obligada a verificar tanto la selección como el nivel de efectividad de los medios técnicos y organizativos utilizados. La exhaustividad de esta verificación debe evaluarse a través del prisma de adecuación a los riesgos y la proporcionalidad en relación con el estado del conocimiento técnico, los costos de implementación y la naturaleza, el alcance, el contexto y los propósitos del tratamiento.

Ciertamente, el principio de responsabilidad previsto en el artículo 28 de la LRJSP, 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, 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. De modo que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, 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" (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, 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".

La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable del tratamiento, que es quien determina la existencia del tratamiento y su finalidad. Recordemos que, las operadoras tratan los datos de sus clientes determinando fines y medios. Por tanto, es responsabilidad de las operadoras (**ORANGE**, en el presente caso) implementar las medidas apropiadas que garanticen el cumplimiento del RGPD, de modo que, si tal principio se ve comprometido debido a la falta de diligencia a la hora de implementar medidas suficientes para ello, se imputará la responsabilidad de tal infracción a la operadora en cuestión.

En este sentido, la Sentencia de la Audiencia Nacional de 9 de febrero de 2023 recoge:

“El principio de culpabilidad derivado del artículo 25CE, según señaló la STC 246/1991, de 19 de diciembre, constituye un principio estructural básico del Derecho administrativo sancionador, y aparece reconocido en el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al disponer que: “Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas o jurídicas (…) que resulten responsables de los mismos a título de dolo o culpa”.

Por eso, como señala la STS de 18 marzo 2005, Rec. 7707/2000, es evidente, «que no podría estimarse cometida una infracción administrativa, si no concurriera el elemento subjetivo de la culpabilidad o lo que es igual, si la conducta típicamente constitutiva de infracción administrativa, no fuera imputable a dolo o a culpa”.

Respecto a que no se habían identificado los riesgos que se ceñían sobre el duplicado de las tarjetas SIM con anterioridad a la aplicación de la Directiva PSD2, cabe señalar que ya en la resolución recurrida se indica -página 872- “En el presente procedimiento, no se está analizando el riesgo existente antes de la aplicación de la llamada PSD2 sino el que se produce a partir de su aplicación, que es cuando se empieza a utilizar el fraude mediante la utilización de un duplicado de una tarjeta SIM obtenido indebidamente por persona distinta de su titular (…) en el presente caso las medidas de seguridad implementadas no resultan suficientes para garantizar la confidencialidad del dato personal en cuestión”

Ahora bien, a mayor abundamiento, resulta claro que el riesgo de suplantación de identidad está presente de manera permanente en la actividad empresarial de (…). Es un riego real con la finalidad última de hacerse pasar por otra persona y que procura, en supuestos como el examinado, la contratación de productos o la obtención de un duplicado de la tarjeta SIM por quien no es el auténtico titular de la misma, riesgo que la recurrente no puede alegar que le resultaba desconocido.

Sobre la supuesta responsabilidad objetiva, la resolución recurrida no considera responsable a (…) por el resultado, sino por una pérdida de confidencialidad vinculada a la insuficiencia de las medidas de seguridad implantadas y, en definitiva, debido a una falta de diligencia de dicha entidad.

(…)

Esa falta de diligencia de (…), como responsable del tratamiento, a la hora de implementar en origen las medidas de seguridad adecuadas para comprobar que la persona que solicita o activa el duplicado de la tarjeta SIM es el titular de ésta es lo que constituye el elemento de la culpabilidad.

En consecuencia, concurre el elemento subjetivo de la culpabilidad necesario para poder sancionar, incompatible con la existencia del error invencible alegado. Las medidas de seguridad implementadas con posterioridad, no afectan a la comisión de la infracción y contrariamente a lo pretendido por la actora no pueden amparar la aplicación de una eximente, sin perjuicio de que hayan sido tomada en consideración como atenuante del artículo 83.2.c) del RGPD a la hora de fijar la sanción.»

Esta Agencia quiere manifestar que, en contra de las alegaciones de **ORANGE**, en las que insiste en que esta Agencia pretende que **ORANGE** prevea todas y cada una de las amenazas que puedan tener lugar, esperando un resultado en que las medidas sean indefectibles, pasando por alto amenazas que difícilmente pueden ser previstas, como sería este caso, el artículo 25 del RGPD determina : "…*el responsable del tratamiento aplicará, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas*…"

Las Directrices 4/2019 del Comité Europeo de Protección de Datos (CEPD) relativas al artículo 25 Protección de datos desde el diseño y por defecto, Versión 2.0, Adoptadas el 20 de octubre de 2020, indican:

"29 El RGPD adopta un enfoque coherente basado en el riesgo en muchas de sus disposiciones, en los artículos 24, 25, 32 y 35, con el fin de determinar las medidas técnicas y organizativas adecuadas para proteger a las personas y sus datos personales y cumplir los requisitos del RGPD. Los bienes protegidos son siempre los mismos (las personas, a través de la protección de sus datos personales), frente a los mismos riesgos (para los derechos de las personas), y teniendo en cuenta las mismas circunstancias (la naturaleza, el ámbito, el contexto y los fines del tratamiento).

> 30. Al realizar el análisis de riesgos para el cumplimiento del artículo 25, el responsable del tratamiento ha de determinar los riesgos que entraña una violación de los principios para los derechos de los interesados, así como su probabilidad y gravedad a fin de aplicar medidas que mitiguen de forma efectiva los riesgos detectados. En las evaluaciones de riesgos es crucial realizar una evaluación sistemática y minuciosa del tratamiento. Por ejemplo, un responsable evalúa los riesgos concretos asociados a la ausencia de un consentimiento libremente otorgado, que constituye una violación del principio de licitud, en el curso del tratamiento de los datos personales de niños y jóvenes menores de 18 años como grupo vulnerable, en un caso en que no existe ningún otro fundamento jurídico, y aplica medidas adecuadas para abordar y mitigar de forma efectiva los riesgos detectados asociados a este grupo de interesados" (el subrayado es nuestros)
>
> En definitiva, el cumplimiento del principio de protección de datos desde el diseño requiere identificar los concretos riesgos para los derechos y libertades de las personas que conlleva el tratamiento, analizarlos y evaluarlos de forma que se permita determinar y aplicar de modo efectivo desde el inicio del tratamiento las medidas técnicas y organizativas específicas para garantizar cada uno de los principios de protección de datos, como los de licitud, exactitud y confidencialidad, lo que en este caso no se ha hecho.
>
> Como ya se señalaba en la contestación a las alegaciones al acuerdo de inicio, se entiende que **ORANGE**, al evaluar los riesgos de la utilización de la aplicación que tiene implantada para emitir duplicados de tarjeta SIM, no ha tenido en cuenta los riesgos, así como su impacto en los derechos y libertades de las personas. Ya ha quedado demostrado que el impacto que este posible riesgo tenía en los derechos y libertades de las personas es alto, y esto tampoco se había tenido en cuenta. Ha sido la falta de diligencia a la hora de implementar en origen las medidas adecuadas para comprobar ***(…)***, precisamente, lo que constituye el elemento de la culpabilidad.

Por lo tanto, procede desestimar la alegación presentada por **ORANGE**.

8.- SOBRE LAS MEDIDAS ADOPTADAS E IMPLEMENTADAS POR ORANGE.

ORANGE vuelve a manifestar que las medidas presentadas a lo largo del procedimiento sancionador no habían sido tenidas en cuenta por parte de esta Agencia, y que, por ello, las vuelve a enumerar. Sin embargo, desde esta Agencia se quiere manifestar que si han sido analizadas y valoradas, y por ello se reproduce lo que se había contestado, tanto en las alegaciones al acuerdo de inicio como en las alegaciones a la propuesta de resolución.

> **"ORANGE** pone de manifiesto que ya habría enumerado las medidas que había desplegado, tanto de manera previa como a posteriori, para que desde esta Agencia se pueda apreciar la constante evolución y análisis de riesgos, así como las medidas aplicadas, teniendo en cuenta la evolución de los supuestos de fraude SIM Swapping.

ORANGE insiste en que tenía establecidas las siguientes medidas:

1. medidas implementadas por **ORANGE** para prevenir la comisión de fraudes derivados de la suplantación de identidad de su cliente.

-documentación ya aportada que se pone a disposición de los agentes y demás personal con capacidad para llevar a cabo actuaciones en **ORANGE**.
-comunicaciones adicionales que reiteran los protocolos de actuación para la emisión de duplicados de tarjeta SIM.
(…).

-**ORANGE** forma parte de la Asociación Española para la Digitalización y participa en el proyecto "Identidad Digital Segura", que tiene por objeto, entre otros, proteger frente al fraude y los ciberataques y la defensa de la privacidad de los datos.
(…).

2. Medidas implementadas por **ORANGE** para prevenir la comisión de fraudes derivados de la suplantación de agentes y/o empleados de **ORANGE**.

-implantación de un doble factor de identificación, que se encontraría en fase de testeo con ciertos usuarios.

-proyecto ***(…)***.

-herramientas de control de tráfico, que es utilizada por el Grupo de Análisis de Riesgos de **ORANGE**, y que puede generar alertas en caso de posibles detecciones de contrataciones irregulares, y que funciona de la siguiente manera en el caso de duplicados de tarjeta SIM:
(…)

3. medidas adoptadas con relación al presente supuesto, no recogidas en los apartados anteriores.

-se ha modificado el riesgo asociado a este tipo de supuestos, ostentando un impacto mayor en los protocolos y actuaciones de la compañía.

-se ha suspendido cautelarmente el ***(…)*** que tiene lugar en los supuestos como el caso que ha motivado la apertura de este procedimiento sancionador, para poder determinar las medidas adecuadas para mitigar los riesgos identificados.

En cualquier caso, **ORANGE** quiere manifestar que lleva a cabo un constante control y revisión de los riesgos existentes en materia de duplicados de tarjeta SIM, que los protocolos se actualizan y que se adoptan medidas acordes a los riesgos identificados, sin que ello permita imponer a las mismas la garantía o exigencia de infalibilidad.

ORANGE manifiesta que desde esta Agencia no se ha revisado este desglose, y entiende que es necesario para comprender la amenaza y poder prevenir y mitigar su comisión, y añade que con ello habría quedado acreditada su

voluntad de protección de los derechos de los particulares, en el que la existencia de un riesgo cero es actualizado y revisado.

Esta Agencia entiende que **ORANGE** sigue manifestando que cumple con las disposiciones del artículo 25 del RGPD. En este caso vuelve a enumerar las medidas que tenía implementadas, y manifiesta que esta Agencia no las ha tenido en cuenta,

Algunas de las medidas puestas de manifiesto por **ORANGE** no resultan de aplicación a supuestos en los que la solicitud de tarjetas SIM se realiza de modo presencial. El tratamiento de los datos no sólo requiere el establecimiento de medidas de ciberseguridad, sino que se hacen necesarias otras medidas para mitigar los riesgos que se derivan ***(…)***.

Alega **ORANGE** que se ha eliminado la posibilidad de realizar duplicados de tarjeta SIM desde el área de clientes, y desde quioscos; se ha puesto en marcha ***(…);*** se ha modificado el riesgo asociado a este tipo de supuestos, ostentando un impacto mayor en los protocolos y actuaciones de la compañía y se ha suspendido cautelarmente ***(…)*** que tiene lugar en los supuestos como el caso que ha motivado la apertura de este procedimiento sancionador, para poder determinar las medidas adecuadas para mitigar los riesgos identificados.

Pues bien, todas estas medidas no se encontraban implementadas por **ORANGE** de forma previa, sino que han sido aplicadas con posterioridad a los hechos, por lo que no se tuvieron en cuenta desde el diseño del tratamiento, por ello no pueden ser tenidas tampoco en cuenta en el presente caso.

En el apartado quinto de la contestación a las alegaciones al acuerdo de inicio se dice, respecto de los documentos aportados por **ORANGE**, lo siguiente:

Se trata de una documentación en la que se hace referencia a la posibilidad de la existencia de riesgos, pero no se identifican de manera concreta, y no se prevén actuaciones en concreto con respecto a la posibilidad de que se produzcan situaciones como la que se ha producido en el presente expediente sancionador, en la medida en que no se hace mención alguna de forma concreta a la posibilidad de que ***(…)***.

No hay ningún documento en el que se prevea cuáles son los riesgos ***(…)***. Ya se ha mencionado en la contestación a estas alegaciones que, desde esta Agencia no se puede considerar que la posibilidad de que los empleados puedan realizar un duplicado de tarjeta SIM no puede ser calificado como bajo, pero esto no implicaría que todos los empleados sean potenciales delincuentes, únicamente que hay que valorar esta posibilidad y tener medidas al respecto, sobre todo teniendo en cuenta cual es el impacto en los derechos y libertades de las personas.

ORANGE manifiesta que, ***(…).***

ORANGE en su escrito de recurso pone de manifiesto que, “entre las medidas técnicas es necesario mencionar el sistema de verificación del DNI, sistema que se

trata de una medida adicional, no predominante de otras medidas, que implica una inversión económica importante en seguridad y cuya manipulación por un agente con mala fe penaliza gravemente frente a esta Agencia a **ORANGE**". En este sentido, **ORANGE** vuelve a dar a entender que no prima en sus medidas de seguridad el riesgo que sus actuaciones puedan producirse a los derechos y libertades de las personas físicas, sino más bien a los de la organización. Ya se ha mencionado en varias ocasiones en el presente expediente que el sistema que tiene implantado para verificar el DNI en los procesos de duplicado de tarjeta SIM no cumple con los requisitos previstos en el artículo 25 del RGPD, y la compañía vuelve a hacer referencia, en este punto, a otros expedientes en los que, según manifiesta, que las medidas implementadas si fueran relevantes. A este respecto, cabe señalar que en dichos expedientes no se hacía referencia al sistema de verificación del DNI en la emisión de duplicados de tarjeta SIM de manera presencial. Por lo que dicha alegación no puede ser tenida en cuenta.

Por todo ello, procede rechazar la alegación presentada por **ORANGE**.

9.- SOBRE LA FALTA DE PROPORCIONALIDAD DE LA SANCIÓN PROPUESTA.

ORANGE en su escrito de recurso pone de manifiesto que habría demostrado que ha actuado con la diligencia debida en los procesos de duplicados de tarjeta SIM. Desde esta Agencia se quiere señalar que ha quedado demostrado que no fue así a lo largo de la resolución que ahora se recurre.

En cualquier caso, también quiere señalar que la sanción impuesta es desproporcionada, y presenta su disconformidad con la valoración de los agravantes, haciendo una argumentación, que ya ha sido analizada en la resolución recurrida de la siguiente manera:

> **"ORANGE** realiza esta afirmación manifestando haber demostrado haber actuado con la diligencia debida en la implementación de medidas en los procesos de duplicados de tarjetas SIM, y que en este supuesto los agentes actuaron de manera individual y dolosa rompiendo los estándares y protocolos de la compañía.
>
> En todo caso, entiende que la sanción incluida en el acuerdo de inicio es desproporcionada atendiendo a las circunstancias y contenido de la supuesta infracción, que **ORANGE** niega.
>
> En relación con el incumplimiento del principio de proporcionalidad, el RGPD prevé expresamente la posibilidad de graduación, mediante la previsión de multas susceptibles de modulación, en atención a una serie de circunstancias de cada caso individual efectivas, proporcionadas y disuasorias (artículo 83.1 y 2 RGPD), condiciones generales para la imposición de las multas administrativas que sí han sido objeto de análisis por esta Agencia, a las que hay que sumar los criterios de graduación previstos en la LOPDGDD.
>
> Hay que señalar que la multa administrativa acordada será efectiva porque

conducirá a la compañía a aplicar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados, habida cuenta del valor de la criticidad del tratamiento.

También es proporcional a la vulneración identificada, en particular a su gravedad, el círculo de personas físicas afectadas y los riesgos en los que se han incurrido y a la situación financiera de la compañía.

Y, por último, es disuasoria. Una multa disuasoria es aquella que tiene un efecto disuasorio genuino. A este respecto, la Sentencia del TJUE, de 13 de junio de 2013, Versalis Spa/Comisión, C-511/11, ECLI:EU:C:2013:386, dice:

"94. Respecto, en primer lugar, a la referencia a la sentencia Showa Denko/Comisión, antes citada, es preciso señalar que Versalis la interpreta incorrectamente. En efecto, el Tribunal de Justicia, al señalar en el apartado 23 de dicha sentencia que el factor disuasorio se valora tomando en consideración una multitud de elementos y no sólo la situación particular de la empresa de que se trata, se refería a los puntos 53 a 55 de las conclusiones presentadas en aquel asunto por el Abogado General Geelhoed, que había señalado, en esencia, que el coeficiente multiplicador de carácter disuasorio puede tener por objeto no sólo una «disuasión general», definida como una acción para desincentivar a todas las empresas, en general, de que cometan la infracción de que se trate, sino también una «disuasión específica», consistente en disuadir al demandado concreto para que no vuelva a infringir las normas en el futuro. Por lo tanto, el Tribunal de Justicia sólo confirmó, en esa sentencia, que la Comisión no estaba obligada a limitar su valoración a los factores relacionados únicamente con la situación particular de la empresa en cuestión."

"102. Según reiterada jurisprudencia, el objetivo del factor multiplicador disuasorio y de la consideración, en este contexto, del tamaño y de los recursos globales de la empresa en cuestión reside en el impacto deseado sobre la citada empresa, ya que la sanción no debe ser insignificante, especialmente en relación con la capacidad financiera de la empresa (en este sentido, véanse, en particular, la sentencia de 17 de junio de 2010, Lafarge/Comisión, C-413/08 P, Rec. p. I-5361, apartado 104, y el auto de 7 de febrero de 2012, Total y Elf Aquitaine/Comisión, C-421/11 P, apartado 82)."

La Sentencia de fecha 11 de mayo de 2006 dictada en el recurso de casación 7133/2003 establece que: "*Ha de tenerse en cuenta, además, que uno de los criterios rectores de la aplicación de dicho principio régimen sancionador administrativo (criterio recogido bajo la rúbrica de «principio de proporcionalidad» en el apartado 2 del artículo 131 de la citada Ley 30/1992) es que la imposición de sanciones pecuniarias no debe suponer que la comisión de las infracciones tipificadas resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas".*

También es importante la jurisprudencia que resulta de la Sentencia de la Sala Tercera del Tribunal Supremo, dictada en fecha 27 de mayo de 2003 (rec.

3725/1999) que dice: *La proporcionalidad, perteneciente específicamente al ámbito de la sanción, constituye uno de los principios que rigen en el Derecho Administrativo sancionador, y representa un instrumento de control del ejercicio de la potestad sancionadora por la Administración dentro, incluso, de los márgenes que, en principio, señala la norma aplicable para tal ejercicio. Supone ciertamente un concepto difícilmente determinable a priori, pero que tiende a adecuar la sanción, al establecer su graduación concreta dentro de los indicados márgenes posibles, a la gravedad del hecho constitutivo de la infracción, tanto en su vertiente de la antijudicidad como de la culpabilidad, ponderando en su conjunto las circunstancias objetivas y subjetivas que integran el presupuesto de hecho sancionable -y, en particular, como resulta del artículo 131.3 LRJ y PAC, la intencionalidad o reiteración, la naturaleza de los perjuicios causados y la reincidencia-. (SSTS 19 de julio de 1996, 2 de febrero de 1998 y 20 de diciembre de 1999, entre otras muchas).*

En este caso, **ORANGE** ponía de manifiesto que había demostrado haber actuado con diligencia en los procesos de duplicados de tarjeta SIM, y que, en este supuesto, los agentes actuaron de manera individual y dolosa rompiendo los protocolos de la compañía.

De este modo, desde esta AEPD se quiere señalar que, en este supuesto, no se está examinando la actuación de los agentes, sino que se está examinando la condición, características y adecuación de las medidas adoptadas por **ORANGE**, y la actuación del responsable del tratamiento al respecto.

ORANGE quiere manifestar su disconformidad en la interpretación que realiza esta Agencia en relación con los agravantes:

a) la naturaleza, gravedad y duración de la infracción (artículo 83.2.a) RGPD.

ORANGE manifiesta que este agravante se apoya en la posible comisión de operaciones bancarias fraudulentas, y considera que no es aceptable jurídicamente utilizar como argumento el uso de las cuentas bancarias, los perjuicios monetarios de las víctimas de los fraudes o el modo en que se llevan a cabo estas operaciones por las entidades financieras para justificar la sanción impuesta, en la medida en que `las entidades bancarias son las únicas responsables de la seguridad de sus operaciones, tal y como afirma la Autoridad Bancaria Europea, en “Opinion on the implementation of the RTS on SCS anf CSC” puntos 37 y 38, y donde se determina que las credenciales de seguridad utilizadas para realizar la autenticación segura de los usuarios de los servicios de pago son responsabilidad de la entidad gestora de servicios de cuenta.

En este sentido, la Agencia considera que la naturaleza de la infracción es muy grave puesto que acarrea una pérdida de disposición y control sobre los datos personales. Ha permitido a los criminales robar la identidad mediante el secuestro del número de teléfono tras obtener un duplicado de su tarjeta SIM. Tras la entrada en vigor de la Directiva PSD2, como se ha indicado, el teléfono móvil ha pasado a desempeñar un rol muy importante en la realización de pagos online al ser necesario para la confirmación de transacciones, y

convierte a este dispositivo -y por extensión a la tarjeta SIM-, en objetivo claro de los ciberdelincuentes.

Conviene señalar que la Directiva PSD2, se aplica a los servicios de pago prestados dentro de la Unión (artículo 2), y no a **ORANGE**, pero también es cierto que la expedición de un duplicado de tarjeta SIM a favor de un tercero que no es el titular de la línea, proporciona a los suplantadores el control de la línea telefónica, y por lo tanto, de los SMS dirigidos al teléfono vinculado a la tarjeta SIM inicial y de esta manera a poder acceder a conocer el código de autentificación de la transacción.

Es cierto que, previamente se han de conocer los datos de acceso a la banca online, pero también es necesario obtener el duplicado de la tarjeta SIM titularidad de la persona a defraudar con la finalidad de hacerse con los SMS de confirmación que el cliente recibirá en su terminal móvil como autentificación de doble factor, y es en esta acción (en la obtención del duplicado) lo que se ha tenido en cuenta en el presente procedimiento sancionador.

En relación con el agravante referido a la infracción del artículo 25 del RGPD **ORANGE** entiende que no habría que tener en cuenta a todos los clientes que tiene, ya que no todos son personas físicas, ni todos solicitan duplicado de la tarjeta SIM. Por ello, entiende que, en este supuesto, solo habría un único implicado que sería la persona que presentó la reclamación.

No obstante, esta Agencia ya ha determinado que la responsabilidad que se le imputa a **ORANGE** es por no contar con las medidas técnicas y organizativas adecuadas para garantizar desde el diseño la protección de datos de los clientes

La Agencia considera que el nivel de los posibles perjuicios es alto, ya que el acceso a los duplicados de dichas tarjetas SIM permite que se realicen operaciones bancarias fraudulentas en un corto espacio de tiempo. Mediante la duplicación de las tarjetas SIM, los supuestos suplantadores pueden conseguir el control de la línea del abonado y con ello la recepción de SMS dirigidos al legítimo abonado para confirmar operaciones on-line con entidades bancarias suplantando su personalidad. Estos SMS los envían las entidades bancarias como parte de la verificación en dos pasos de operaciones como transferencias monetarias o pagos por Internet, y el acceso a estos SMS suele ser el motivo de la duplicación fraudulenta de las tarjetas SIM.

Es cierto que **ORANGE** no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias ni se le puede atribuir la responsabilidad por fraude bancario. No obstante, también es cierto que, si **ORANGE** asegurase el procedimiento de identificación y entrega, ni siquiera podría activarse el sistema de verificación de las entidades bancarias. La persona estafadora tras conseguir la activación de la nueva SIM, toma el control de la línea telefónica, pudiendo así, a continuación, realizar operaciones bancarias fraudulentas accediendo a los SMS que las entidades bancarias envían a sus clientes. Esta secuencia de hechos genera una serie de daños y perjuicios graves que deberían haberse tenido en cuenta en una evaluación de

impacto relativa a la protección de datos (considerando 89, 90, 91 y artículo 35 del RGPD) o en el análisis de riesgos correspondiente. En definitiva, desde el momento que se entrega un duplicado a una persona distinta a la titular de la línea o persona autorizada, el cliente pierde el control de la línea y los riesgos, daños y perjuicios, se multiplican. Además, los hechos acontecen con una inmediatez abrumadora.

En suma, la aplicación del artículo 83.2.a) del RGPD se refiere a la gravedad de los Hechos Probados, que se pone de manifiesto, entre otras cuestiones, en la alarma social generada por la realización de estas prácticas fraudulentas y por la altísima probabilidad de materialización del riesgo, sin que sea determinante el número de reclamaciones presentadas. Y ello, porque lo que se ha analizado en el presente procedimiento sancionador son las medidas técnicas y organizativas implantadas por el responsable del tratamiento a raíz de la reclamación presentada ante la AEPD.

En relación a la manifestación de **ORANGE** referida a que no todos los clientes tomados en consideración en el acuerdo de inicio para fijar el número de afectados son personas físicas, señalar que esta Agencia ha tomado el dato de su página web, y que puede aportar el dato del número de clientes que son personas físicas, aunque como ya se ha señalado, en la aplicación del artículo 83.2.a) se ha tenido en cuenta el número de clientes, pero también la alarma social generada por la realización de estas prácticas fraudulentas y por la altísima probabilidad de materialización del riesgo, y sin que sea determinante el número de reclamaciones presentadas

b) toda infracción anterior cometida por el responsable o encargado del tratamiento (artículo 83.2.e RGPD)

ORANGE pone de manifiesto que no deberían tenerse en cuenta las infracciones previas cometidas y sancionadas, ya que no guardan relación con el presente supuesto. No obstante, el apartado e) del artículo 83.2 del RGPD recoge expresamente “toda infracción anterior cometida por el responsable”, por lo que dentro de la misma entrarían todos los supuestos que se han reflejado en el acuerdo de inicio, teniendo en cuenta que en ningún momento se indica que tales infracciones deban ser la misma que el caso en cuestión.

c) la vinculación entre la actividad empresarial de la reclamada y el tratamiento de datos personales de clientes o de terceros (artículo 83.2.k RGPD en relación con el artículo 76.2.b) LOPDGDD.)

ORANGE manifiesta que este factor es ambiguo en su valoración para incluirlo como agravante, ya que dicha vinculación no supone una relación directa con la supuesta infracción, y, además, exige que dicho agravante sea puesto en relación con el supuesto de hecho concreto, y por tanto que el tratamiento de datos no nace de una intención de la entidad, sino que tiene lugar la comisión de un delito.

Sin embargo, desde esta Agencia se tiene en cuenta que el desarrollo de la actividad empresarial que desempeña **ORANGE** requiere un tratamiento

continuo y a gran escala de los datos personales de los clientes, entre el que se incluye la emisión de duplicados de tarjeta SIM, **ORANGE** se configura como una de las grandes operadoras de telecomunicaciones de nuestro país. Resulta obvio que la actividad de **ORANGE** implica necesariamente la realización de un alto número de operaciones de tratamiento de datos personales de las personas físicas clientes de dicha entidad, lo que repercute en la diligencia que debe desplegar en el cumplimiento de las obligaciones derivadas de este tratamiento de datos.

Además, no puede olvidarse que este supuesto de hecho concreto se produce por una falta de medidas técnicas y organizativas adecuadas por parte de **ORANGE**.

Por último, añadir que el legislador es quien previó la posibilidad de utilizar este agravante y que la Agencia se limita a aplicarla.

d) intencionalidad o negligencia en la infracción.

ORANGE manifiesta que esta Agencia no relaciona este agravante, ni señala su aplicación al presente supuesto de hecho.

De este modo, entiende que, según ha manifestado el TJUE cuando manifestaba que la imposición de sanciones coercitivas por la autoridad administrativa solo es admisible en los casos en los que se aprecie una conducta culpable por el responsable o encargado del tratamiento, la imposición de este agravante debe estar reservado a los casos en los que la intencionalidad o negligencia sea evidente o grave.

Por ello, en este caso, en el que el supuesto viene causado por un acto delictivo no imputable a **ORANGE**, entiende que no debería imputarse este agravante sin razonamiento alguno al respecto.

En lo que respecta a que el supuesto de hecho que ha motivado la apertura de este expediente sancionador viene causado por un hecho delictivo no imputable a **ORANGE**, se reitera lo ya manifestado en esta propuesta de reolución en lo referente a que lo que se imputa a **ORANGE** es el hecho de no tener implementadas las medidas necesarias para que no se produzca el duplicado de la tarjeta SIM en los términos en los que se ha producido. En este sentido, si **ORANGE** hubiera sido diligente a la hora de implementar las medidas adecuadas para la emisión de los duplicados de tarjetas SIM no se habría producido un supuesto como el que comunicaba la parte reclamante.

Además, se considera que la conducta de **ORANGE** responde al tipo infractor y al título de culpa, considerándose que ha actuado con negligencia grave en la infracción del artículo 25. 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 la aplicación de las medidas técnicas y organizativas adecuadas, estas suplantaciones de identidad se hubieran podido evitar.

Si bien la Agencia considera que no hubo intencionalidad por parte de **ORANGE**, concluye que fue negligente al no asegurar un procedimiento que garantizase la protección de los datos personales de los clientes. De manera que se produce un resultado socialmente dañoso que impone la desaprobación de las medidas implantadas que resultaban ineficaces, independientemente del nivel de compromiso demostrado, que resulta incuestionable.

Negar la concurrencia de una actuación negligente por parte de **ORANGE** equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no compartimos esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida. Una gran empresa que realiza tratamientos de datos personales de sus clientes a gran escala, de manera sistemática y continua, debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos, tal y como establece la jurisprudencia.

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 en continuo tratamiento de datos de clientes, 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".*

En este sentido, es de vital importancia establecer e implantar los procedimientos y medidas necesarios, en función de las características y entidad de la operadora, que permitan demostrar que se ha tenido una debida diligencia a la hora de intentar evitar que se produjese una suplantación de identidad. Además, se ha de poder demostrar que se han adoptado las necesarias precauciones durante el desarrollo de la actividad empresarial, exigidas por la normativa, para evitar un daño que fuera previsible. Se trata de tener un nivel de cuidado objetivo atendiendo a las concretas circunstancias del caso que posibilite hacer patente que se estaba al tanto de la posibilidad de sufrir una suplantación de identidad, y que, con ello, se aplicaron las medidas oportunas para reducir la concreción de tal riesgo al mínimo posible.

Asimismo, sobre la aplicación de esta circunstancia como agravante se ha pronunciado la Audiencia Nacional en su SAN de uno de marzo de dos mil veinticuatro (Núm. de Recurso: 0001757 /2021) en la que considera que procede la aplicación de la circunstancia contemplada en el artículo 83.2.b) del RGPD en el caso de falta de diligencia de entidades que realizan tratamientos de datos a gran escala, así se especifica que *"(…) Y en este sentido se debe señalar que una empresa como la demandante que realiza tratamientos de*

datos personales de sus clientes a gran escala, de manera sistemática y continúa debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos. La actora pone el acento en la ausencia de intencionalidad cuando el precepto habla también de negligencia y es en esa falta de diligencia en la que pone el acento la resolución recurrida en relación con ambas infracciones (…)"

Por tal motivo, se considera justificada la aplicación de la circunstancia contemplada en el artículo 83.2.b) del RGPD.

Por otro lado, **ORANGE** manifiesta que se deberían haber tenido en cuenta las siguientes atenuantes:

-la parte reclamada procedió a bloquear la línea en cuanto tuvo conocimiento de los hechos. (art. 83.2.c).

No se puede tener en cuenta este atenuante, cuando, como consecuencia de la infracción imputada, la parte reclamante ha sufrido pérdidas que ascienden a los 9.000 euros.

-no se han tratado categorías especiales de datos (art. 83.2.g).

No se puede tener en cuenta esta alegación en la medida en que tratar datos personales incluidos dentro de la categoría de datos especiales se puede tener en cuenta como agravante para el cálculo de la sanción, pero nunca tratar datos de carácter personal que no estén incluidos dentro de esta categoría puede ser considerada como atenuante, a la hora de imponer una sanción.

Además, se tiene en cuenta que la tarjeta SIM es un dato personal que tiene una naturaleza especialmente sensible, ya que posibilita la suplantación de identidad.

-el grado de cooperación de **ORANGE** con la AEPD. De este modo, **ORANGE** quiere manifestar que ha quedado acreditado que se ha contestado en tiempo y forma a todos los requerimientos de información solicitados, con el fin de poner remedio a una supuesta infracción y mitigar sus posibles efectos adversos (art. 83.2.f).

No se puede tener en cuenta esta alegación en la medida en que contestar a los requerimientos de información enviados desde esta Agencia son una obligación del responsable, tal y como se recoge en la LOPDGDD.

-la adhesión a códigos de conducta en virtud del artículo 40 o mecanismos de certificación aprobados con arreglo al artículo 42 (art. 83.2.j)

ORANGE aporta como documento nº 15 un certificado emitido por AENOR, por el que se acredita que **ORANGE** tiene aprobado desde el 4 de septiembre de 2023 un sistema de cumplimiento normativo que cumple con los requisitos del artículo 31 bis del Código Penal, así como el resto de estándares de cumplimiento e materia de prevención de delitos, como la Circular 1/2016, de

22 de enero, de la Fiscalía General del Estado, destinado a la mitigación de cualquier riesgo de comisión de delitos en el marco de la actuación de **ORANGE**.

Esta certificación no puede ser tenida en cuenta a la hora de fijar los poderes correctivos, pues no se trata, en este caso, de acreditar que se han adoptado medidas de cumplimiento normativo en materia penal, sino de acreditar que se cumplen estándares en materia de protección de datos.

-el inexistente beneficio obtenido por **ORANGE** en el tratamiento de los datos que ocupa este procedimiento sancionador, añadiendo que, en todo caso, sería perjudicada, como ya se ha señalado, siendo parte perjudicada en el procedimiento penal en el que se denuncia la comisión del delito que nos ocupa (83.2.k).

Esta alegación presentada por **ORANGE** no puede ser tenida en cuenta, en la medida en que, el hecho de que no se hayan obtenido beneficios no puede ser considerado como un atenuante, de acuerdo con la sentencia de la Audiencia Nacional, de 05/05/2021, rec. 1437/2020, que indica: *"Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante"; aplicado al supuesto enjuiciado, la falta del presupuesto para su aplicación respecto del art. 76.2.c) de la LOPDGDD, esto es, obtener beneficios consecuencia de la infracción, no permite su aplicación como atenuante."*

De este modo, conforme a lo previsto en el artículo 83.1 del RGPD, admitir la ausencia de beneficios como una atenuante, no solo es contrario a los presupuestos de hechos contemplados en el artículo 76.2.c), sino también contrario a lo establecido en el artículo 83.2.k) del RGPD y a los principios señalados.

Así, valorar la ausencia de beneficios como una atenuante anularía el efecto disuasorio de la multa, en la medida en que minora el efecto de las circunstancias que inciden efectivamente en su cuantificación, reportando al responsable un beneficio al que no se ha hecho merecedor. Sería una rebaja artificial de la sanción que puede llevar a entender que infringir la norma sin obtener beneficios, financieros o del tipo que fuere, no le producirá un efecto negativo proporcional a la gravedad del hecho infractor.

En todo caso, las multas administrativas establecidas en el RGPD, conforme a lo establecido en su artículo 83.2, se imponen en función de las circunstancias de cada caso individual y no se estima que la ausencia de beneficios sea un factor de graduación adecuado y determinante para valorar la gravedad de la conducta infractora. Solo en el caso de que esta ausencia de beneficios sea

relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora podrá considerarse como una atenuante, en aplicación del artículo 83.2.k) del RGPD, que se refiere a “cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso”.

Por todo ello, procede desestimar la presente alegación.

III
Conclusión

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

IV
Resolución extemporánea

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

De acuerdo con lo establecido en el art. 24 de la LPACAP el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

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

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

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **ORANGE ESPAGNE, S.A.U.** contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 22 de octubre de 2024, en el expediente EXP202213023.

SEGUNDO: NOTIFICAR la presente resolución a **ORANGE ESPAGNE, S.A.U.**.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea notificada la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en el Banco

CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

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

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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

1245-21112023

Olga Pérez Sanjuán
La Subdirectora General de Inspección de Datos, de conformidad con el art. 48.2 LOPDGDD, por vacancia del cargo de Presidencia y Adjuntía