PI24-006

RESOLUCIÓN Nº R25-041 DEL PROCEDIMIENTO DE INFRACCIÓN Nº PI24-006

Por la Autoridad Vasca de Protección de Datos se ha instruido el expediente de infracción PI24-006, derivado de los expedientes AP23-001 y DN23-054 por la actuación del Departamento de Seguridad del Gobierno Vasco, y en base a los siguientes

ANTECEDENTES DE HECHO

PRIMERO: Con fecha 12 de septiembre de 2023 la Autoridad Vasca de Protección de Datos tuvo conocimiento de la difusión por diferentes canales de internet y redes sociales de un documento con una batería fotográfica formada por setenta y nueve fotografías, correspondientes a personas detenidas por su presunta implicación en la comisión de delitos de robo con violencia e intimidación durante el transcurso de la pasada Aste Nagusia de Bilbao, por lo que acordó la apertura de unas actuaciones previas para clarificar los hechos y determinar si se había producido una vulneración de la normativa de protección de datos.

SEGUNDO: Con fecha 5 de octubre de 2023 tuvo entrada en el Registro General de la Autoridad Vasca de Protección de Datos (AVPD), escrito de denuncia remitido por la Agencia Española de Protección de Datos, en el que se ponía en conocimiento de esta Autoridad hechos que podían constituir una infracción de la normativa sobre protección de datos de carácter personal. En dicho escrito se manifestaba lo siguiente:

> *«En el canal de Telegram https://t.me[...] se han publicado unas supuestas fichas policiales con los nombres y las fotografías de unos presuntos detenidos durante las pasadas fiestas de Bilbao. Presuntamente está información ha sido obtenida de la Policía Municipal de Bilbao y de la Ertzaintza.*
>
> *La publicación concreta se encuentra aquí: https://t.me/[...]*
>
> *Esta "información" ha sido ya publicada por varios medios de comunicación https://www.esdiario.com/espana/[...]*
>
> *https://www.edatv.news/noticias/[...]*
>
> *Mediante esta denuncia solicito a la AEPD que verifique si efectivamente se ha filtrado tal "información", investigue si las administraciones públicas afectadas han sufrido una brecha de seguridad, y sancione a todos los actores que proceda.*
>
> *Se solicita expresamente que en la investigación también se incluya al ciudadano […], ya que el tratamiento de datos que realiza no es a título individual, como persona física, sino como parte de una actividad económica. Él se denomina creador de contenidos, percibe ingresos por los mismos y además solicita donaciones vía patreon e incluye un número de cuenta bancaria en su perfil de Telegram.»*

A dicho escrito se acompañaba diversa documentación consistente en dos archivos en formato "Pdf": "DOCUMENTO CON LAS SUPUESTAS FICHAS POLICIALES" y "PUBLICACIÓN DE […] CERTIFICADA DIGITALMENTE"; documentos que junto con el escrito de denuncia han quedado incorporados al expediente.

TERCERO: Con fecha 23 de noviembre de 2023 tuvo entrada en esta Autoridad Vasca de Protección de Datos escrito del Departamento de Seguridad del Gobierno Vasco presentando contestación al requerimiento realizado por esta Autoridad con fechas 9 de octubre y 9 de noviembre de 2023, en el que se manifestó lo siguiente:

> *"En relación al interés mostrado por parte de la Agencia Vasca de Protección de Datos respecto del tipo de investigaciones seguidas con ocasión del presente asunto -la filtración en diferentes canales de Internet de fotografías, identidades y posible relación de determinadas personas con infracciones penales-, cabe informar que tales hechos fueron puestos en conocimiento de la autoridad judicial, instruyéndose a tal efecto el atestado policial de referencia […]. Dichas diligencias policiales fueron remitidas a la autoridad judicial en fecha […], dando lugar a las Diligencias Previas […] que se siguen en el Juzgado de Instrucción Nº 7 de Bilbao.*
>
> *Cabe significar que continúan desarrollándose las investigaciones de cuyo resultado se dará cuenta al órgano judicial. En este sentido, algunas de estas indagaciones policiales derivan de los rastros y registros informáticos que permitan advertir la trazabilidad de la filtración y difusión acaecida. En la actualidad, sentimos no poder ofrecer información adicional en la medida que la investigación, tutelada por la autoridad judicial, no ha finalizado y una mayor concreción de las actuaciones practicadas pudiera comprometer el resultado de la misma".*

CUARTO: Con fecha de 18 de diciembre de 2023 se solicitó al Ministerio Fiscal para que informara si los hechos objeto de las diligencias previas nº […] en curso en el Juzgado de Instrucción nº7 de Bilbao eran coincidentes con los hechos denunciados ante esta Autoridad Vasca de Protección de Datos.

QUINTO: Con fecha de 23 de febrero de 2024 tuvo entrada en el registro de la Autoridad Vasca de Protección de Datos Decreto del Ministerio Fiscal indicando que dicha información debía solicitarse al Juzgado de Instrucción nº 7 de Bilbao.

SEXTO: Con fecha 28 de febrero de 2024 se remitió escrito a Juzgado de Instrucción nº 7 de Bilbao en el que se preguntaba si los hechos objeto de las diligencias previas […] en curso en su Juzgado eran coincidentes con los hechos denunciados ante esta Autoridad Vasca de Protección de Datos.

SÉPTIMO: Con fecha 4 de marzo de 2024 tuvo entrada en esta Autoridad Vasca de Protección de Datos escrito del Juzgado de Instrucción nº 7 de Bilbao, presentando contestación a la solicitud en la que se indicó que:

> *"Visto el contenido de la petición recibida de la Autoridad Vasca de Protección de Datos, trasládese que, con los datos ofrecidos en la comunicación remitida, resulta sumamente probable que el documento al que se hace referencia, sea coincidente con el que se relaciona con el asunto penal objeto de instrucción en las presentes diligencias previas".*

OCTAVO: Con fecha 11 de marzo de 2024 por el Presidente de la Autoridad Vasca de Protección de Datos se acordó iniciar procedimiento de infracción al Departamento de Seguridad del Gobierno Vasco por una presunta infracción del principio de integridad y confidencialidad establecido en el artículo 5.1 f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de protección de datos o RGPD), y suspender el procedimiento incoado hasta que recayese resolución judicial firme.

NOVENO: Con fecha 9 de octubre de 2024 se recibió en la Autoridad Vasca de Protección de Datos providencia del Juzgado de Instrucción nº7 de Bilbao en el que se pone en conocimiento de esta autoridad de control la firmeza del Auto de 23 de mayo de 2024 por el que se acuerda el sobreseimiento provisional de la causa.

DÉCIMO: Con fecha de 23 de octubre de 2024 el Presidente de la Autoridad Vasca de Protección de Datos acordó levantar la suspensión del procedimiento de infracción incoado al Departamento de Seguridad del Gobierno Vasco por una presunta vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1 f) del Reglamento General de Protección de Datos,

DECIMOPRIMERO: Con fecha de 25 de noviembre de 2024 se recibió en la Autoridad Vasca de Protección de Datos escrito del Departamento de Seguridad del Gobierno Vasco en el que se recogía lo siguiente:

«Con fecha 24 de octubre de 2024 se ha recibido Acuerdo de levantamiento de suspensión del Procedimiento de infracción de ref.: PI24-006, seguido en la citada Autoridad por una presunta vulneración del artículo 5.1. f) del Reglamento General de Protección de Datos. A tal respecto, y a la vista de la información que se desprende de las actuaciones de investigación realizadas por nuestra organización, desde la Dirección de Coordinación de Seguridad del Departamento de Seguridad, se realizan las siguientes consideraciones:

Con fecha 5 de septiembre de 2023, esta Dirección de Coordinación de Seguridad puso en conocimiento de la Autoridad Vasca de Protección de Datos que el 30 de agosto de 2023, personal de la Ertzain-etxea de Bilbao, había tenido conocimiento de la difusión por diferentes canales de internet y redes sociales de uso común, de un documento policial. El documento publicitado se componía de una batería, formada por setenta y nueve fotografías con los nombres y apellidos de personas consideradas de interés policial por su presunta implicación en la comisión de delitos de robos con violencia e intimidación, en el ámbito de actuación de la Ertzain-etxea de Bilbao.

Por otro lado, la organización policial pudo advertir que el contenido del documento coincidía con uno de los informes elaborados, para Aste Nagusia de 2023, por parte de una sección (OLI) adscrita a la Ertzain-etxea de Bilbao.

El documento publicado en redes sociales constaba de cinco páginas, en formato PDF, con una marca de agua en todas sus páginas con la inscripción "TME […]". Esta misma mención figuraba en la cabecera del documento y, bajo la misma, además, se reflejaba el título siguiente: "BATERÍA FOTOGRÁFICA INDIVIDUOS MAS ACTIVOS EN LA COMISIÓN DE ROBOS CON VIOLENCIA~INTIMIDACIÓN".

Asimismo, cabe significar que tan pronto fueron conocidos tales hechos, desde nuestra organización se activaron diversas y paralelas acciones al objeto de averiguar la naturaleza y dimensión del incidente, así como la autoría del mismo, para depurar las responsabilidades que, en su caso, pudiesen corresponder. En particular, cabe anticipar que las acciones consistieron en:

- *La apertura de la investigación interna para conocer el origen del archivo y las personas autoras de su filtración-difusión.*

- *La solicitud cursada a distintas redes sociales habituales peticionando la eliminación del citado archivo.*

- *La comunicación de los hechos a la Fiscal Superior del País Vasco.*

Efectivamente, a la vista de lo acontecido, y dentro del ámbito competencial de la Jefatura de Asuntos Internos (JAI), como mecanismo de control del cumplimiento de las órdenes establecidas en el marco del deber de sigilo, se iniciaron las correspondientes diligencias de investigación tendentes a la persecución de los hechos, adoptando las medidas indagatorias pertinentes para que se dedujeran responsabilidades, tanto en ámbito penal como disciplinario, que, en su caso, pudiera haber lugar.

Tal y como informa la JAI, su investigación pudo determinar que "[…]" se correspondería con el seudónimo utilizado por […], persona que habitualmente despliega una importante actividad en distintas páginas web y redes sociales. Además de la citada persona, otros canales habituales de difusión (TikTok, Instagram, WhatsApp...) se hicieron rápidamente eco de la noticia y contribuyeron a difundir el documento.

De otro lado, de manera inmediata, el mismo día 1 de setiembre de 2023, tras tener conocimiento de la información que se estaba divulgando y la afección que podía acarrear a las personas que en la misma aparecían (incluso a la propia eficacia de la labor policial), desde la Jefatura de Investigación Criminal y Policía Judicial de la Ertzaintza, se establecieron los mecanismos oportunos para solicitar su retirada de estas redes sociales.

Por su parte, la JAI siguió las líneas de investigación tendentes a determinar la procedencia y la identidad de la persona o personas que hubieran contribuido a su filtración y/o difusión.

De tales actuaciones de investigación, según refieren, se pudo desprender que el documento y las diferentes fotos había sido elaborado en origen por la OLI y almacenado en un directorio al que únicamente tenían acceso el personal policial adscrito a la citada sección de la Comisaría, así como la propia Jefatura de la Ertzain-etxea.

Según se desprende de las declaraciones efectuadas en la investigación, dicha sección, en el marco de las funciones que tiene atribuidas, y a fin de facilitar la labor preventiva de los recursos de Protección Ciudadana, sobre las 13:00 horas del día 24 de agosto de 2023, difundió el documento, vía correo electrónico, a través del canal corporativo de la Ertzaintza, a las direcciones que de manera normalizada habían sido establecidas por la Jefatura para el traslado de este tipo de informaciones, todo ello en el marco de las funciones propias que tendrían asignadas cada uno de estos receptores.

Asimismo, y al tiempo que se establecían esas primeras medidas de contención citadas anteriormente, desde la Jefatura de División de Investigación Criminal de la Ertzaintza, se

pusieron los hechos en conocimiento de la Fiscalía Superior del País Vasco, para su conocimiento y efectos que por su parte estimase oportunos.

Precisamente, en fecha 4 de octubre de 2023, la AVPD fue informada, desde nuestra Dirección, de que el acceso y difusión del contenido de dicho archivo en las redes sociales generalistas, se había visto significativamente interrumpido fruto de las gestiones realizadas por parte de nuestro Departamento en el momento inicial de los hechos. Asimismo, se indicaba al órgano de control que proseguían las actuaciones de investigación iniciadas en su momento, habiéndose puesto en conocimiento de la Fiscal Superior del País Vasco los hechos referidos, cuyo atestado policial […] dio lugar a las Diligencias Previas […] seguidas en el Juzgado de Instrucción nº 7 de Bilbao.

En el marco de la investigación que se estaba llevando a cabo por la JAI, nuestra organización realizó una serie de gestiones de comprobación en el ámbito informático que, en su caso, pudieran ser de interés para conocer la trazabilidad del archivo e intentar así determinar la autoría de la posible difusión de tales datos.

En este sentido, de las gestiones realizadas en el marco de dicha investigación y de la información facilitada por los servicios informáticos (Dirección General de Telecomunicaciones y Sistemas Informáticos -DGTSI-), se extrajeron una serie de conclusiones.

En relación con el control de accesos y extracciones de información del servidor, a nivel informático no se audita el acceso de lectura ni el copiado a otros dispositivos, únicamente se recogía la información de creación, modificación o borrado de los documentos en carpetas de Unidades en red.

En cualquier caso, con ocasión de las presentes alegaciones, nuestra organización considera necesario significar que, para tratar de garantizar el nivel de confidencialidad de la información sensible contenida en estos documentos policiales, técnicamente se establece una primera restricción de acceso a la información, asignando perfiles informáticos a cada usuario. Es por ello que, en este caso, solamente tuvieron acceso al documento los perfiles de personal usuario debidamente autorizado para elaborar, modificar o tratar el documento.

Por otro lado, en relación a la difusión del documento a través de correo electrónico, se adjuntaba una tabla con información sobre los buzones a los que se habría trasmitido el archivo con la cadena "batería fotográfica" en el asunto, es decir, cualquier mensaje que se hubiera enviado o recibido vía correo electrónico dentro del canal corporativo con el asunto. En este sentido, se observaba que, en un primer momento, la información se cursó a través del canal corporativo al personal debidamente autorizado por razón de su cargo o funciones encomendadas, todo ello, en el marco de las necesidades intrínsecas de garantizar la seguridad de un evento de la magnitud de la Aste Nagusia.

Por ello, el documento se envió, además de a la Jefatura de la Ertzain-etxea de Bilbao, a los responsables de las secciones de investigación y a los teléfonos corporativos de los recursos de Protección Ciudadana, con los datos necesarios para garantizar una identificación rápida y eficaz de las personas responsables de la comisión de este tipo de hechos delictivos: fotografía, filiación...

A este respecto, consideramos oportuno advertir que, técnicamente, los teléfonos corporativos asignados a los recursos de Protección Ciudadana disponen de una

restricción, consistente en que se imposibilita el reenvío de este tipo de documentos policiales a terminales externos fuera del entorno policial.

Asimismo, se constató que desde algunos buzones de correo electrónico se reenvió la información dentro del canal corporativo y siguiendo las funciones que tenían atribuidas. No obstante, desde la DGTSI se indicaba que cuando una operación sent no tiene operaciones received a continuación se puede concluir que ha sido enviada a algún buzón externo, si bien la auditoria no recoge los datos de las direcciones de destino. Por tanto, sobre esta cuestión se pudo dar fe de que diversos usuarios habrían enviado el documento PDF fuera del canal corporativo, sin embargo, con los datos auditados por los servicios informáticos, resultaba imposible conocer fehacientemente el número de usuarios que habrían reenviado el archivo, pues el hecho de que otros usuarios difundieran el documento a través del canal corporativo provocaba que, automáticamente, se registrara a continuación una operación RECEIVED y, por tanto, no se podía descartar que alguno de ellos también pudiera haber reenviado al mismo tiempo el documento a algún usuario fuera del canal corporativo, ya que esta acción no quedaría registrada.

Por último, cabe señalar que los agentes que enviaron el archivo fuera del canal corporativo alegaron que esta acción se realizó en el marco de un interés meramente laboral y negaban haber filtrado el documento fuera del entorno policial. En cualquier caso, resultaba totalmente imposible constatar fehacientemente que alguno de ellos, o cualquier otro ertzaina, pudiera haber difundido el documento. Además, con la información recogida en la investigación, se pudo detectar que, debido a las necesidades intrínsecas de la labor policial, la información se expandió de forma exponencial, resultando imposible un control posterior de la trazabilidad de la misma. Todo ello, se recogió en las conclusiones finales remitidas en el atestado […] al juzgado de instrucción nº 7 de Bilbao, en fecha 18 de enero de 2024.

Finalmente, cabe señalar que, mediante Auto de fecha 23 de mayo de 2024, se acordó el sobreseimiento provisional de la causa penal.

Llegados a este punto, nuestra organización considera importante significar las siguientes cuestiones:

a) *En origen, el tratamiento con fines policiales de los datos contenidos en el documento publicitado, resultaba legítimo y adecuado en el marco de la prevención y protección de la seguridad pública, especialmente en un evento de la magnitud de la Aste Nagusia y al amparo de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.*
   Efectivamente, el tratamiento de tales datos (nombre apellidos y fotografía) y el flujo de la información entre el personal policial y recursos policiales intervinientes, a priori, se antoja necesario, adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados. Es más, por el contrario, no se advierte otro tratamiento diferente que permitiese lograr la finalidad pretendía (prevención y protección de la seguridad ciudadana). Téngase presente, la naturaleza y dimensión del evento festivo de la Aste Nagusia de Bilbao, así como los incidentes y antecedentes delictivos que suelen ser frecuentes y persisten durante tales fechas festivas.

b) *Nuestra organización dispone de diversas medidas de índole organizativas y técnicas destinadas a garantizar la protección de la información contenida en nuestro Sistema de Información Policial.*

Sin perjuicio de las previsiones legales (Decreto Legislativo 1/2020, de 22 de julio, por el que se aprueba el texto refundido de la Ley de Policía del País Vasco, así como su régimen disciplinario) relativas al deber de secreto y sigilo que resulta de completa aplicación al colectivo policial, se debe sumar distinta normativa interna que impone el deber de adoptar medidas que garanticen la confidencialidad y seguridad de los datos personales y que eviten el acceso y uso de los datos no autorizado. En este sentido, igualmente cabe traer a colación la formación que se imparte en distintos cursos de promoción y especialización, así como la intervención de la JAI, no únicamente en el marco de la depuración de responsabilidades, sino igualmente en la faceta de concienciación, difundiendo «Notas Informativas» que coadyuven a una praxis correcta en el desempeño de la actividad policial y en particular de la obligación de sigilo profesional.

A mayor abundamiento, se deben destacar aquellas medidas técnicas que ofrece el Sistema de Información Policial. En relación al supuesto que nos ocupa, nos encontramos con:

- *una definición de perfiles informáticos del personal usuario que permite delimitar el acceso a la información;*
- *un canal corporativo por el que se facilita la información;*
- *la utilización de teléfonos corporativos asignados a los recursos de Protección Ciudadana que imposibilitan el reenvío de documentos policiales como el que nos ocupa a terminales externos fuera del entorno policial.*

c) *Asimismo, se debe tener presente que el Departamento ha actuado en todo momento de forma ágil y diligente a la hora de:*

- *por un lado, comunicar los hechos a la AVPD, así como a la Fiscal Superior del País Vasco;*
- *por otro lado, activar los mecanismos oportunos para solicitar la retirada del documento de las redes sociales -donde no parece que resulte atribuible a personal de nuestra organización la difusión de la información en tales redes sociales-,*
- *y, finalmente, practicar las correspondientes investigaciones que derivaron en el procedimiento penal seguido por estos hechos.*

d) *Dicho lo anterior, entendemos que, en el presente caso, no cabe aplicar una responsabilidad directa al Departamento de Seguridad. Existe jurisprudencia (Sentencia 188/2022 de 15 febrero de 2022 del Tribunal Supremo, Sala de lo Contencioso-administrativo, Sección 3ª) que establece que la obligación que recae sobre el responsable de la actividad de tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos personales no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas que, conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado.*

Efectivamente, consideramos que el Departamento de Seguridad, además de actuar con especial agilidad a la hora de gestionar la difusión no autorizada, tiene implementadas medidas adecuadas que se han utilizado con una diligencia razonable.»

DECIMOSEGUNDO: Con fecha de 20 de diciembre de 2024 se recibió en la Autoridad Vasca de Protección de Datos nuevo escrito del Departamento de Seguridad del Gobierno Vasco en el que se alegó lo siguiente:

"En relación al procedimiento de infracción PI24-006 tramitado por la Autoridad Vasca de Protección de Datos (AVPD), desde nuestro Departamento de Seguridad se ha estimado oportuno completar los elementos de respuesta facilitados por la Dirección de Coordinación de Seguridad en fecha 22 de noviembre de 2024, con información adicional que puede, si así lo considera la AVPD, resultar de interés a la tramitación del presente expediente.

La información facilitada por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos (DGTSI) -responsable los sistemas de la seguridad y de la explotación, según la política de seguridad de la información (PSI)-, concreta algunas de las características tecnológicas comunicadas en aquel escrito de alegaciones, respecto de las medidas de seguridad y protección de los datos, que, en el ámbito policial, se encuentran implementadas en el sistema, canal o dispositivos corporativos.

En este sentido, se pone de manifiesto que:

- *Se encuentran establecidas diferentes medidas de seguridad que, de forma alineada con los requisitos del Esquema Nacional de Seguridad y de la Protección de Datos, permiten disponer de controles adecuados en la protección de la información. Dichas medidas se organizan en un marco organizativo a través de la citada PSI y sus Comités de Seguridad, un marco operativo estructurado en una Normativa de Seguridad de obligado cumplimiento para todo el personal que accede a las redes, sistemas y aplicativos del Departamento de Seguridad del Gobierno Vasco (DSGV) y un marco de medidas concretas para determinados sistemas como el Sistemas de Información Policial (SIP).*
- *Las peculiaridades de la información policial imponen medidas específicas que aseguren su confidencialidad, disponibilidad, integridad y trazabilidad a lo largo de todo su ciclo de vida.*
- *La información vinculada al SIP no estructurada como ficheros, videos, etc. se almacena en repositorios centralizados con control de acceso establecido de forma restrictiva que limita el mismo a grupos determinados gestionados a través del Directorio Activo del DSGV. No está autorizado, ni técnicamente se permite, el almacenamiento de información en los discos locales de los equipos y la extracción de la misma a dispositivos externos está limitada a determinados perfiles de usuarios y controlada a través de mecanismos de DLP (Data Leak Prevention) que identifican el movimiento de información de carácter personal o documentos de carácter policial.*
- *La integridad de la dicha información no estructurada se asegura mediante el despliegue de mecanismos antivirus y réplicas de la información.*

- *La trazabilidad de los accesos a los sistemas, documentos, correo electrónico, etc., se asegura mediante el software […]. Este permite identificar quién, cuándo y desde dónde ha accedido a los repositorios de información y a los buzones de correo. Los accesos al Sistema de Informática Policial (SIP) se controlan por la auditoría de la propia aplicación. Dada su criticidad, el propio sistema de auditoría cuenta con medidas de seguridad que impiden el acceso a la información registrada a personal no autorizado.*
- *Respecto a la disponibilidad, el DSGV dispone de infraestructuras redundantes y configuraciones de los sistemas que permiten asegurar el acceso a los sistemas con mínimos tiempos de indisponibilidad."*

DECIMOTERCERO: Con fecha 3 de febrero de 2025, el Presidente de la Autoridad Vasca de Protección de Datos ordenó la sustitución de la persona instructora del procedimiento PI24-006 incoado al Departamento de Seguridad del Gobierno Vasco.

DECIMOCUARTO: Con fecha 13 de febrero de 2025, por el instructor del procedimiento se adoptó propuesta de resolución en el sentido de apercibir al Departamento de Seguridad del Gobierno Vasco por vulneración del principio de integridad y confidencialidad recogido en el artículo 6.1 f) de la Ley Orgánica 7/2021, conducta constitutiva de una infracción prevista en el artículo 58 b) del mismo cuerpo legal.

DECIMOQUINTO: La propuesta de resolución fue notificada a la Administración reclamada el día 18 de febrero de 2025.

DECIMOSEXTO: Con fecha 12 de marzo de 2025, tuvo entrada en esta Autoridad escrito del Director de Coordinación de Seguridad, en el que se expone lo siguiente:

"[…] A tal efecto, sirva la presente para ratificar y reiterarnos en todo lo manifestado en las alegaciones vertidas durante la tramitación del presente procedimiento, debiéndose subrayar, a modo de conclusión:

a) En origen, la comunicación y el tratamiento con fines policiales de los datos contenidos en el documento publicitado, resultaba legítimo y adecuado en el marco de la prevención y protección de la seguridad pública, especialmente en un evento de la magnitud de la Aste Nagusia y al amparo de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

b) El Departamento ha actuado en todo momento de forma ágil y diligente a la hora de comunicar los hechos a la AVPD, así como a la Fiscal Superior del País Vasco; activar los mecanismos oportunos para solicitar la retirada del documento de las redes sociales y practicar investigaciones tendentes a la averiguación de los hechos, así como de la persona autora.

c) Sin perjuicio de las previsiones legales y de normativa interna que, relativas al deber de secreto y sigilo, están obligados a atender los miembros de la Ertzaintza, nuestra organización dispone de diversas medidas de índole organizativas y técnicas destinadas a garantizar la protección de la información contenida en nuestro Sistema de Información

Policial y a que el tratamiento de tales datos se realice por personal autorizado para el cumplimiento de sus funciones.

Por tanto, consideramos que, en el presente caso, la comunicación ilícita de datos personales a terceros no autorizados, que desembocó en una difusión en redes sociales, no deviene directamente de una quiebra de las medidas técnicas u organizativas implementadas, y por tanto no debiera atribuirse a nuestra organización la responsabilidad sobre la vulneración del principio de confidencialidad o la pérdida del control de los datos."

HECHOS PROBADOS

De la documentación obrante en el expediente se constata que:

- El 30 de agosto de 2023, personal de la Ertzain-etxea de Bilbao, había tenido conocimiento de la difusión por diferentes canales de Internet y redes sociales de uso común, de un documento policial. El documento publicitado se componía de una batería, formada por setenta y nueve (79) fotografías con los nombres y apellidos de personas consideradas de interés policial por su presunta implicación en la comisión de delitos de robo con violencia e intimidación, en el ámbito de actuación de la Ertzain-etxea de Bilbao. Esta difusión fue puesta en conocimiento de la AVPD con fecha 12 de septiembre de 2024 por la Dirección de Coordinación de Seguridad del Departamento de Seguridad del Gobierno Vasco.
- El documento publicado en redes sociales consta de cinco páginas, en formato PDF, con una marca de agua en todas sus páginas con la inscripción "TME […]". Esta misma mención figuraba en la cabecera del documento y, bajo la misma, además, se reflejaba el título siguiente: "BATERÍA FOTOGRÁFICA INDIVIDUOS MAS ACTIVOS EN LA COMISIÓN DE ROBOS CON VIOLENCIA~INTIMIDACIÓN".
- La organización policial reconoce que el contenido del documento y las diferentes fotos han sido elaborados en origen por una sección (OLI) adscrita a la Ertzain-etxea de Bilbao para la Aste Nagusia de 2023, y almacenado en un directorio al que únicamente tenían acceso el personal policial adscrito a la citada sección de la Comisaría, así como la propia Jefatura de la Ertzain-etxea
- Que dicha sección de la Ertzain-etxea de Bilbao, en el marco de las funciones que tiene atribuidas, y a fin de facilitar la labor preventiva de los recursos de Protección Ciudadana, sobre las 13:00 horas del día 24 de agosto de 2023, difundió el documento, vía correo electrónico, a través del canal corporativo de la Ertzaintza, a las direcciones que de manera normalizada habían sido establecidas por la Jefatura para el traslado de este tipo de informaciones, todo ello en el marco de las funciones propias que tendrían asignadas cada uno de estos receptores.
- Que por la Dirección General de Telecomunicaciones y Sistemas Informáticos –(DGTSI) se pudo dar fe de que diversos usuarios corporativos con acceso autorizado al documento policial y a las diferentes fotos habrían enviado el documento PDF fuera del canal corporativo, sin que sea posible conocer fehacientemente el número de usuarios que habrían reenviado el archivo, ya que la auditoria no recoge los datos de las direcciones de destino. Según se reconoce en la investigación policial realizada a nivel interno, los agentes que

enviaron el archivo fuera del canal corporativo alegaron que esta acción se realizó en el marco de un interés meramente laboral y negaban haber filtrado el documento fuera del entorno policial.

FUNDAMENTOS DE DERECHO

I

Se formula la presente Resolución de acuerdo con lo previsto en el artículo 39 de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos en relación con el artículo 44 de la Ley 1/2023, de 16 de marzo, de la potestad sancionadora de las Administraciones Públicas Vascas.

II

Según los hechos probados, la normativa aplicable al tratamiento realizado por la Ertzaintza consistente en la elaboración del documento policial y las diferentes fotos así como el tratamiento ulterior, es la recogida en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (artículos 2 y 4).

La Ley Orgánica 7/2021, al igual que lo hace el RGPD, define en su artículo 5 los datos personales como toda información sobre una persona física identificada o identificable y define, a su vez el tratamiento como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

El principio de integridad y confidencialidad recogido en el artículo 5.1 f) del RGPD tiene también su reflejo casi exacto en la Ley Orgánica 7/2021, concretamente en el artículo 6.1 f) y es uno de los principios relativos al tratamiento. Los principios relativos al tratamiento son el punto de partida y la cláusula de cierre del ordenamiento jurídico de protección de datos, constituyendo verdaderas reglas informadoras del sistema con una intensa fuerza expansiva.

El artículo 6.1 f) de la Ley Orgánica 7/2021 define dicho principio estableciendo que "*los datos personales serán tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas*".

Tal y como se expone en la relación de hechos probados, corroborados por la propia Administración en sus alegaciones, el documento policial y las fotografías difundidas en redes sociales fueron elaborados por la sección OLI adscrita la Ertzain-etxea de Bilbao, y aun no habiéndose determinado en la investigación policial ni judicial qué personal de la Ertzaintza comunicó a terceros no autorizados dicha información, sí se

reconoce que se envió por correo electrónico a destinatarios que no formaban parte del correo corporativo de la organización policial.

Por lo tanto, se ha producido un tratamiento de datos de carácter personal en los términos definidos por el artículo 5 de la Ley Orgánica 7/2021, dado que se permitió el acceso a datos personales de terceros sin autorización ni legitimación.

El artículo 6.1 f) de la Ley Orgánica 7/2021 impone que los datos personales sean tratados de forma que se garantice una seguridad adecuada de los mismos, incluida, entre otros, la protección contra el tratamiento no autorizado o ilícito mediante la aplicación de medidas técnicas u organizativas apropiadas.

La citada normativa contiene una regla que afecta a la confidencialidad como parte de la seguridad de los datos de carácter personal, tratando de salvaguardar el derecho de las personas a mantener la privacidad de tales datos y, en definitiva, el poder de control o disposición sobre los mismos. En este sentido, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos por parte de quienes están en contacto con los datos personales.

La infracción del deber de confidencialidad es una infracción de resultado que obliga no sólo al responsable del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento, de forma que lo relevante es que se vulnere la confidencialidad de los datos cuya custodia corresponde al responsable; esto es, lo relevante es que esa información que estaba obligado a guardar en virtud del deber de secreto llegó a manos de terceros.

En este sentido, la Sala de lo Contencioso Administrativo del Tribunal Supremo en la sentencia nº 10007/2019, de 8 de julio, señala lo siguiente:

> "*En efecto, procede recordar que, según una doctrina consolidada del Tribunal Constitucional y de este Tribunal Supremo, toda la información de carácter personal de los ciudadanos que las Administraciones Públicas recoge y almacena, ha de ser estrictamente necesaria e imprescindible para el ejercicio de las potestades que le atribuya la ley y ha de ser, asimismo, adecuada para procurar alcanzar las legítimas finalidades previstas en las normas, de modo que las autoridades públicas son responsables de garantizar que no se divulguen datos personales que no sean absolutamente necesarios para el ejercicio de funciones públicas, con el objeto de preservar de forma real y efectiva los derechos fundamentales protegidos en el artículo 18 de la Constitución*".

El considerando 28 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y cuya trasposición en España se llevó a cabo con la aprobación de la citada Ley Orgánica 7/2021, establece:

> *"Con el fin de mantener la seguridad del tratamiento y evitar que con él se infrinja lo dispuesto en la presente Directiva, los datos personales deben ser tratados de modo que se garantice un nivel adecuado de seguridad y confidencialidad, en particular impidiendo el acceso sin autorización a dichos datos o el uso no autorizado de los mismos y del equipo utilizado en el tratamiento, teniendo en cuenta el desarrollo técnico existente y la*

tecnología, los costes de ejecución con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse."

Y es que como recoge el considerando 51 de la citada Directiva 2016/680, los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales, en particular cuando el tratamiento pueda dar lugar, entre otros, a la **pérdida de confidencialidad de datos sujetos al secreto profesional**.

En tal sentido el considerando 60 de la Directiva 2016/680 establece:

"Al objeto de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en la presente Directiva, el responsable o el encargado del tratamiento deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida ***la confidencialidad****, teniendo en cuenta el estado de la técnica, el coste de su aplicación con respecto al riesgo y la naturaleza de los datos personales que deban protegerse. En la evaluación de los riesgos relacionados con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos, como la destrucción accidental o ilícita, la pérdida, la alteración,* ***la comunicación no autorizada o el acceso no autorizado a datos personales transmitidos, almacenados o sometidos a cualquier otro tipo de tratamiento****, que puedan ocasionar, en particular, perjuicios físicos, materiales o inmateriales.* ***El responsable*** *y el encargado del tratamiento* ***deben asegurarse de que el tratamiento de datos personales no lo llevan a cabo personas no autorizadas****."*

La Administración en sus alegaciones al acuerdo de levantamiento de la suspensión, tal y como se ha recogido en el antecedente decimosegundo, concreta y amplia la información sobre las medidas de seguridad y protección de los datos, que, en el ámbito policial, se encuentran implementadas en el sistema, canal o dispositivos corporativos de la organización policial.

Y en las alegaciones a la propuesta de resolución, la Administración reclamada se ratifica y reitera en las alegaciones vertidas durante la tramitación del procedimiento y concluyen que el tratamiento en origen del documento publicitado resultó legítimo y adecuado al amparo de la Ley Orgánica 7/2021, que reaccionó de forma ágil y diligente a la hora de comunicar los hechos a la AVPD y a la Fiscal Superior del País Vasco, activando los mecanismos para la retirada del documento publicitado en redes sociales y practicando investigaciones para averiguar la autoría de los hechos, y que disponen de diversas medidas de índole organizativas y técnicas destinadas a garantizar la protección de la información contenida en el Sistema de Información Policial. Y esto le lleva a la Administración reclamada a considerar que la comunicación ilícita de datos personales a terceros no autorizados no deviene de una quiebra de las medidas técnicas u organizativas implementadas y por tanto no debiera atribuirse a la Administración la responsabilidad sobre la vulneración del principio de confidencialidad o la pérdida de control de datos.

Pero estas alegaciones no pueden ser estimadas. En el presente caso se ha vulnerado el principio de confidencialidad pues consta que hubo por parte del responsable del tratamiento una comunicación no autorizada o ilícita de datos personales a terceros

no autorizados que desembocó en una difusión en redes sociales, lo que supuso la pérdida de confidencialidad y de control de datos personales, como son los nombres y apellidos y fotografías de los afectados, siendo ello un resultado objetivo, reconocido por el responsable, que no una responsabilidad objetiva. La organización policial reconoce que el contenido del documento y las diferentes fotos han sido elaborados en origen por una sección (OLI) adscrita a la Ertzain-etxea de Bilbao para la Aste Nagusia de 2023.

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

La vulneración del principio de integridad y confidencialidad del artículo 6.1 f) de la Ley Orgánica 7/2021 [artículo 4.1 f) de la Directiva 2016/680] constituye una infracción prevista en el artículo 58 b) de la Ley Orgánica 7/2021.

De conformidad con el artículo 62 de la citada Ley Orgánica, en caso de que el sujeto responsable sea alguno de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo.

Por tanto, en virtud de lo dispuesto en el artículo 77.2 de la LOPDGDD procede declarar dicha infracción al Departamento de Seguridad del Gobierno Vasco, apercibiéndole por la misma.

Por todo lo cual, vistos los preceptos citados, la Ley 1/2023, de 16 de marzo, de la potestad sancionadora de las Administraciones Públicas Vascas, y demás normativa de general y pertinente aplicación, el Presidente de la Autoridad Vasca de Protección de Datos

RESUELVE

PRIMERO. - APERCIBIR al Departamento de Seguridad del Gobierno Vasco por vulneración del principio de integridad y confidencialidad recogido en el artículo 6.1 f) de la Ley Orgánica 7/2021, conducta constitutiva de una infracción prevista en el artículo 58 b) del mismo cuerpo legal.

SEGUNDO. - REQUERIR al Departamento de Seguridad del Gobierno Vasco para que adopte las medidas organizativas internas tendentes a evitar en el futuro situaciones como las referidas en este procedimiento, y para que notifique a la Autoridad Vasca de Protección de Datos dichas medidas en el plazo de un mes desde la notificación de la resolución.

TERCERO: Notificar la presente resolución a la parte reclamante y al Departamento de Seguridad del Gobierno Vasco.

CUARTO: Comunicar la presente resolución al Ararteko de conformidad con lo establecido en el artículo 28.8 de la 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

La presente resolución agota la vía administrativa y frente a la misma podrán las partes interponer recurso potestativo de reposición ante el Presidente de la Autoridad Vasca de Protección de Datos en el plazo de un mes a contar desde el día siguiente al de su notificación (artículos 123 y 124 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas), o directamente recurso contencioso-administrativo ante el Juzgado de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente al de la notificación de este acto (artículos 8.3 y 46 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa).

Vitoria-Gasteiz, a 10 de abril de 2025

78893858V UNAI ABERASTURI (R: Q0100547I)

Firmado digitalmente por 78893858V UNAI ABERASTURI (R: Q0100547I)
Fecha: 2025.04.10 14:20:53 +02'00'

DATUAK BABESTEKO EUSKAL AGINTARITZA
AUTORIDAD VASCA DE PROTECCIÓN DE DATOS

Unai Aberasturi Gorriño
Presidente de la Autoridad Vasca de Protección de Datos