Expediente N.º: EXP202211394

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: La Agencia Española de Protección de Datos tuvo conocimiento a través de una denuncia presentada por **FUNDACIÓN ÉTICAS DATA SOCIETY** (en adelante, la denunciante) de ciertos hechos que susceptibles de vulnerar la legislación en materia de protección de datos.

En virtud de tal conocimiento, en fecha 27 de octubre de 2022, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación previstas en el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), con el fin de investigar a la **SECRETARÍA DE ESTADO DE SEGURIDAD, DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS, DEL MINISTERIO DEL INTERIOR** con NIF S2816001H (en adelante, la parte investigada) con relación a los mencionados hechos.

SEGUNDO: Como consecuencia de ello la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones y potestades asignadas a las autoridades de control por los artículos 48.1 a) y 50 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. (en adelante LO 7/2021), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los extremos que seguidamente se exponen.

El contenido de la denuncia presentada giraba en torno al Sistema de Seguimiento Integral de los casos de Violencia de Género (Sistema VioGén) de la Secretaría de Estado de Seguridad del Ministerio del Interior. Dicho sistema consiste en una aplicación web diseñada para coordinar las actuaciones de los profesionales públicos españoles que se encargan del seguimiento, asistencia y protección de las mujeres denunciantes de violencia de género y de sus hijos.

A través del escrito, la denunciante manifiesta en particular que el Sistema VioGén:

(…).

CUARTO: Con fecha 19 de octubre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 20 de la LO 7/2021 y del artículo 35 de la LO 7/2021, tipificadas correlativamente en el artículo 59.e) d y 59.l) de la misma norma.

QUINTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la parte reclamada presentó escrito donde se formulaban diversas alegaciones en los términos y con el contenido que más abajo se expone.

SEXTO: Con fecha 13 de marzo de 2024 se formuló por la presente autoridad propuesta de resolución, en la cual se procedió al análisis y contestación de las mencionadas alegaciones, finalizando con la propuesta de declaración de las siguientes infracciones imputables a la parte reclamada

- Infracción del artículo 20 de la LO 7/2021, tipificada en el artículo 59 f
- Infracción del artículo 35 de la LO 7/2021, tipificada en el artículo 59.e)
- Infracción del artículo 41 de la LO 7/2021, tipificada en el artículo 59.l)

Asimismo, siguiendo lo dispuesto en el artículo 77.1 de la LOPDGDD, en caso de confirmarse la infracción en la resolución que se adopte, se proponía la adopción, en el plazo de tres meses, de las siguientes medidas:

- Incluir la información en materia de protección de datos exigida por el artículo 21 de la LO 7/2021 en todos aquellos documentos y/o diligencias facilitadas a las víctimas en el momento en que se vayan a tratar sus datos personales, de forma que se cumpla de forma efectiva la obligación prevista en el artículo 20 de dicha norma.

- La realización y superación de la Evaluación de Impacto de Datos personales en los términos y con el contenido mínimo exigido por el artículo 35 LO 7/2021.

- Implementar las medidas necesarias con el fin de garantizar la autonomía e independencia del DPD y evitar, de esta forma, cualquier situación que le origine un conflicto de intereses.

En dicha propuesta se ponía de manifiesto el procedimiento a fin de que en el plazo de quince días hábiles pudiera alegar cuanto considere en su defensa y

presentar los documentos e informaciones que considerase pertinentes, de acuerdo con el artículo 89.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (en adelante, LPACAP)

SÉPTIMO: La práctica de dicha notificación se realizó de forma electrónica, en los términos establecidos por los artículos 40 y siguientes de la LPACAP, poniéndose a disposición en fecha 13/03/2024 tal y como queda acreditado en el acuse de recibo que consta en el expediente administrativo. No obstante, al transcurrir diez días naturales desde dicha fecha sin que se accediese a su contenido por parte de su destinatario, la misma se entendió rechazada en fecha 24/03/2024, dándose por efectuado el trámite y siguiéndose el procedimiento, como preceptúan los artículos 41.5 y 43.2 de la LPACAP.

OCTAVO: Notificado la citada propuesta conforme a las normas establecidas en la LPACAP y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada. Procede, en consecuencia, proseguir las actuaciones mediante la emisión de la presente resolución que, una vez notificada, pondrá fin al procedimiento sancionador, sin perjuicio de los recursos que, en su caso, proceda interponer.

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

HECHOS PROBADOS

PRIMERO: A través de la diligencia realizada por el inspector actuante durante el transcurso de las actuaciones de investigación realizadas en fecha 28/02/2023 se hizo constar que a través del acceso a la URL ***URL.1 que se encuentra dentro de la página web del Ministerio de Interior se accede a una página que ofrece los siguientes apartados relacionado con la Violencia contra la mujer:

- *“Sistema VioGén*
- *Supresión de Datos Sistema VioGén*
- *Noticias y Eventos*
- *Marco Jurídico*
- *Publicaciones*
- *Estadísticas del sistema Viogén*
- *Enlaces de interés”*

“El Sistema de Seguimiento Integral en los casos de Violencia de Género (Sistema VioGén), de la Secretaría de Estado de Seguridad del Ministerio del Interior, se puso en funcionamiento el 26 de julio del 2007, en cumplimiento de lo establecido en la Ley Orgánica 1/2004, de 28 de diciembre, "de Medidas de Protección Integral contra la Violencia de Género", siendo sus objetivos:

- *Aglutinar a las diferentes instituciones públicas que tienen competencias en materia de violencia de género*
- *Integrar toda la información de interés que se estime necesaria*
- *Hacer predicción del riesgo*
- *Atendiendo al nivel de riesgo, realizar seguimiento y protección a las víctimas en todo el territorio nacional*
- *Efectuar una labor preventiva, emitiendo avisos, alertas y alarmas, a través del "Subsistema de Notificaciones Automatizadas", cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima.*
- *Buscando, finalmente, establecer una tupida red que permita el seguimiento y protección de forma rápida, integral y efectiva de las mujeres maltratadas, y de sus hijos e hijas, en cualquier parte del territorio nacional.”*

De igual forma, por lo que se refiere al apartado “supresión de datos Sistema VioGén” en virtud de la citada diligencia, ha quedado constatado que aparece la siguiente información:

- *“El Sistema VioGén (Sistema de Seguimiento Integral de los Casos de Violencia de Género) es un tratamiento de datos de carácter personal cuyo responsable es la persona titular de la Dirección General de Coordinación y Estudios del Ministerio de Interior.*
- *Este tratamiento desarrolla las actividades necesarias para garantizar la seguridad y protección de las víctimas de violencia de género, facilitar el seguimiento de las medidas aplicadas y prevenir actividades delictivas vinculadas a la violencia de género con la finalidad de proteger a dichas víctimas y prevenir infracciones penales sobre las mujeres que se puedan ser sujetos pasivos de tales conductas.*

- *Las personas que se consideran interesadas en este fichero serán las víctimas de hechos susceptibles de ser tipificados como violencia de género y las personas incursas en procedimientos e investigaciones judiciales relacionadas con esos mismos hechos, sin que dicha inclusión prejuzgue el derecho a la presunción de inocencia, cuestión ésta que será dirimida por las Autoridades Judiciales competentes.*

- *La información sobre este fichero y toda la relativa a la forma de ejercer los derechos por parte de los interesados se puede obtener en extenso en la página web.*

- *Dada la finalidad de este tratamiento y su descripción, en correspondencia con los derechos fundamentales susceptibles de ponderación, en cuanto al ejercicio del derecho de supresión, cabe señalar que los datos registrados en el Sistema VioGén serán conservados de conformidad con el artículo 8 de la LOPDP y sólo serán suprimidos a instancia de las personas interesadas en aquellos casos que exista una resolución judicial firme de sobreseimiento definitivo, una sentencia absolutoria firme y se cancelen los antecedentes penales (judiciales) derivados de las mismas.*

- *Pudiendo, no obstante, ser denegadas aquellas solicitudes de supresión de datos cuando los mismos sigan siendo necesarios para la consecución de los fines para los que fueron recabados (protección a las víctimas y prevención de infracciones penales relacionadas con violencia de género), o cuando haya habido cualquier reiteración, reincidencia o quebrantamiento de las medidas judiciales o las penas. Sin perjuicio de aplicar el artículo 24 de la LOPDP si fuese necesario y estuviera motivado el aplicar alguna restricción a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.*

- *En relación con lo señalado resulta ineludible aportar la documentación compulsada que acredite la firmeza de las resoluciones y la finalización de los procedimientos (Sentencia absolutoria, archivo, sobreseimiento o ejecutoria de cumplimiento de condena (para estos casos requiere la acreditación previa de cancelación de antecedente penal).*

- *Los formularios podrán presentarse, para validación y registro preceptivo, ante cualquier dependencia de Policía Nacional o Guardia Civil, así como ante cualquier oficina de las Delegaciones o Subdelegaciones del Gobierno, existentes en cada provincia, a través del Registro Electrónico General de la Administración General del Estado de acuerdo a lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas).*

- *Las solicitudes se responderán en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se podría prorrogar el plazo otros dos meses más (lo cual será trasladado al interesado).”*

Al clicar el link *“página web”* del párrafo cuarto del texto transcrito queda igualmente acreditado que aparecen los siguientes apartados:

- *“Normativa aplicable*
- *Cómo ejercer sus derechos*
- *Registro de Actividades de Tratamiento*
- *Delegados de Protección de Datos del Ministerio del Interior”*

Asimismo, en dicha página se encuentran los siguientes documentos disponibles para descargar en formato pdf:

- *“Formulario de ejercicio de los derechos de protección de datos de carácter personal para el Sistema de Seguimiento integral de los Casos de Violencia de Género.*
- *Formulario general para ejercicio de los derechos de protección de datos de carácter personal (no valido para antecedentes policiales)*
- *Registro de actividades de tratamiento del Ministerio de Interior”*

Queda acreditado que al seleccionar el apartado “*Cómo ejercer sus derechos”* se muestra la siguiente información:

- *“Las personas interesadas podrán ejercer los derechos de acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del Reglamento General de Protección de datos, y los derechos de acceso, rectificación, supresión y limitación conforme a los artículos 20 a 25 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.

- *Cada Centro Directivo del Ministerio del Interior podrá indicar, en su sede o sección web correspondiente, procedimientos particulares para ejercer los derechos.*

- *CÓMO EJERCER SUS DERECHOS SOBRE ANTECEDENTES POLICIALES Para ejercer los derechos relacionados con los antecedentes policiales se ha establecido un procedimiento particular, disponible en la página Gestión de Antecedentes policiales.*

- *CÓMO EJERCER EL RESTO DE DERECHOS DE TRATAMIENTOS DEL MINISTERIO DEL INTERIOR Para aquellos tratamientos que no disponen de un procedimiento particular, de manera general se pueden ejercer los derechos de la siguiente manera:*

    - *En primer lugar, debe descargarse el Formulario general para ejercicio de los derechos de protección de datos de carácter personal (no válido para antecedentes policiales ni violencia de género) que tiene disponible al final de esta página, en la sección de DESCARGAS.*

    - *Como excepción, para ejercer los derechos relacionados con el Sistema de Seguimiento Integral de los Casos de Violencia de Género, siga el mismo procedimiento, teniendo en cuenta que el formulario a descargar y rellenar es el Formulario de ejercicio de los derechos de protección de datos de carácter personal para VioGén, que tiene disponible en la sección de DESCARGAS, al final de esta página (Información sobre el sistema VioGén).*
    - *Cumplimente el formulario adecuado debidamente, especificando cual es el tratamiento sobre el cual desea ejercer sus derechos (Responsable de tratamiento y Nombre del tratamiento) y qué derecho(s) desea ejercer. Los datos necesarios para identificar al tratamiento concreto en el formulario (Nombre del tratamiento y Responsable del tratamiento) puede obtenerlos en el documento Registro de Actividades de Tratamiento, disponible en el apartado DESCARGAS, en el que se listan los distintos tratamientos del Ministerio, agrupados por Centro Directivo.*

- *No se admitirán aquellos formularios incompletos en que no se identifiquen debidamente el responsable de tratamiento, el nombre del tratamiento y los derechos que se desean ejercer.*

- *Una vez debidamente cumplimentado el formulario, se puede remitir al responsable de Tratamiento por dos vías diferentes:*
  - *A través del Registro electrónico, remitiendo el formulario a través del procedimiento existente en la sede electrónica del Ministerio del Interior (requiere tener un Certificado Digital y poder realizar Firma electrónica mediante applet Java o aplicación Autofirma).*
  - *O presencialmente a través de la red de oficinas de asistencia en materia de registros, presentando el formulario en papel.*

- *No se admitirán solicitudes que vengan por otros medios (cómo por ejemplo correo postal o correo electrónico).*

- *También tiene derecho a reclamar ante la Agencia Española de Protección de Datos: C/ Jorge Juan, 6. 28001. MADRID (www.aepd.es)"*

Dentro del documento relativo al Registro de actividades de tratamiento del Ministerio del Interior, cuya última actualización es de fecha 29/09/2023, se establece como responsable del tratamiento del Sistema VioGén a la Secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios. (en adelante, SEGDGCE)

SEGUNDO. La parte reclamada aportó durante las actuaciones de investigación el *"protocolo de primer contacto policial con víctimas de violencia de género en situación de desprotección (protocolo cero)"*.

Dentro de dicho documento, el cual forma parte del expediente administrativo del presente procedimiento se encuentra la siguiente información relativa al primer contacto policial con víctimas de violencia de género:

- *"Las ocasiones en las que el personal de las FFCCS actuante que se encuentra en la primera línea de intervención con víctimas de violencia de género obtienen o pueden obtener información a través de manifestaciones de las personas en el lugar de los hechos y de su observación directa de gran interés para mejorar la posterior valoración policial del riesgo y de esta forma activar en las mejores condiciones el Protocolo Policial y todas las ulteriores acciones que se pueden desprender de manera complementaria para aumentar de forma integral la protección de las víctimas y atender a sus necesidades conforme a lo dispuesto en la Instrucción SES 4/2019. La información que, en muchas ocasiones, obtienen quienes realizan estas intervenciones, muy guiadas en términos de inmediatez, puede resultar clave en la mejora de los procedimientos que deben dirigirse a la protección de las víctimas especialmente vulnerables, limitando que se pierda información mediante un protocolo estructurado que oriente de forma clara en tareas importantes. De esta forma, la*

Guía de Actuación del Protocolo Cero en Violencia de Género describe acciones muy específicas durante el primer contacto policial con víctimas de violencia de género mediante los siguientes ejes:

- *Durante el proceso de intervención policial se deberán tener en cuenta, especialmente, todos los aspectos relacionados con la seguridad de la víctima y de menores, en el caso de que los hubiera.*

- *Las actuaciones operativas y documentales enmarcadas en este Protocolo Cero están especialmente indicadas para los supuestos en los que el personal policial ha sido informado por la víctima de su negativa a denunciar formalmente en dependencias policiales, o tengan indicios de ello, sobre las circunstancias que motivaron hechos presuntamente relacionados con un suceso de violencia de género, ya sean conocidos por primera vez o relacionados con un quebrantamiento de medidas judiciales.*

- *La fuerza actuante deberá prestar especial atención a las manifestaciones de las personas que se hallen en el lugar de los hechos, especialmente de la víctima, conforme a los indicadores y escenarios de riesgo recogidos en la Guía de Actuación anexada en esta instrucción. En este sentido, dispondrán de un documento de trabajo elaborado al efecto denominado Guía de Actuación del Protocolo Cero en Violencia de Género.*

- *Durante la intervención policial, quienes actúan deberán valorar el momento más adecuado, si resulta oportuno, para oír a la víctima en lo que quiera manifestar y en su caso aclarar respecto a las circunstancias que motivaron los presuntos hechos delictivos. En estos supuestos, se deberá obtener la información posible en un entorno privado, lejos de menores como de cualquier otra persona. Se debe aprovechar para conocer si precisa de recursos asistenciales específicos.*

- *En el caso de existir menores a cargo de la víctima, el personal policial deberá constatar si los presuntos hechos se han producido en su presencia y si en esta u otra ocasión han sufrido agresiones y/o amenazas directas o indirectas.*

- *Antes de abandonar el lugar de la intervención, quienes actúan en primera instancia deberán informar a la víctima de los teléfonos y recursos próximos disponibles. En especial de aquéllos que ofrecen atención inmediata y confidencialidad."*

Queda acreditado que en el Anexo de dicho Documento se desarrolla la Guía de Actuación del Protocolo Cero en Violencia de Género en el primer contacto con la víctima de violencia de género. En el mismo se indican las siguientes recomendaciones:

- *"Las siguientes recomendaciones constituyen un decálogo que va a permitir obtener información de gran valor para posteriormente poder evaluar el riesgo de la víctima de violencia de género y conocer mejor aspectos de vulnerabilidad y desprotección. Está especialmente orientado a los casos en los que existan indicios de que, al menos inicialmente, la víctima no quiera presentar denuncia. Para ello, se precisa de su observación como agentes actuantes y de la información obtenida de la víctima, el presunto agresor o de cualquier persona que pueda facilitar información de interés en el contexto de la intervención en el ámbito de la violencia de género.*

  - *Solicite información de la víctima en un entorno privado, alejada tanto de menores como de cualquier otra persona. Aproveche también para conocer si precisa de recursos asistenciales específicos.*
  - *Intente obtener información a través de todas las fuentes disponibles mediante las manifestaciones de las personas presentes y de su observación (víctima, testigos, presunto agresor, otros).*
  - *Tenga cuidado al obtener la información, priorizando la seguridad de la víctima y de menores. Tenga también en cuenta que la preocupación de la víctima por su propia seguridad puede afectar a su capacidad para proporcionar la información necesaria.*
  - *Preste atención al entorno y a las personas que están presentes. Confíe en la experiencia de situaciones similares.*
  - *En el caso de que la intervención policial se desarrolle en un domicilio preste atención al entorno para conocer en qué medida le puede aportar información útil y valiosa.*
  - *En ningún momento sugiera el sentido de las respuestas en los supuestos en los que sea recomendable y pertinente realizar alguna pregunta. Realizar las preguntas a cualquier persona informante con habilidad y educación.*

- *Tenga en cuenta que el momento más peligroso es cuando el presunto autor descubre que la víctima podría intentar terminar la relación.*
- *Pueden existir otros indicadores o circunstancias que ayudan en la predicción de una nueva agresión. Indíquelo cuando corresponda.*
- *Intente conocer si hay menores afectados o en situación de vulnerabilidad.*
- *No abandone el lugar sin informar a la víctima de los teléfonos y recursos próximos disponibles. En especial de aquéllos que ofrecen atención inmediata y confidencialidad."*
- *"Esta Guía de Actuación para sucesos de violencia de género se enmarca en un procedimiento denominado Protocolo Cero que está orientado a mejorar las actuaciones de los agentes policiales en el lugar de los hechos y especialmente indicado para los supuestos de actuación policial con víctimas de un presunto delito de violencia de género en el que, por distintas circunstancias, exista sospecha de que la víctima no acuda a prestar declaración en dependencias policiales. Por su inmediatez, la información obtenida en el lugar de la actuación es de gran valor debido a la carencia de información para realizar la valoración policial de riesgo que existe en algunos casos. Recuerde la importancia de esta información debido a que el principal objetivo de este «protocolo de contacto» es garantizar la recogida de un mínimo de información de forma rápida y directa que permita mejorar la cumplimentación posterior de la Valoración Policial del Riesgo (VPR) y así poder ajustar mejor el riesgo potencial de la víctima y conocer su nivel de vulnerabilidad. Por tanto, este documento incorpora un decálogo de recomendaciones concretas relacionadas con la información disponible en cada momento y situación. "*

- *"Debido a las singulares circunstancias de este tipo de intervenciones y al escenario de riesgo en el que se pueden encontrar las víctimas especialmente vulnerables, en la media de lo posible, trate de interiorizar las recomendaciones incluidas en esta guía de actuación para poder comparecer con el máximo detalle tras la actuación en el lugar de los hechos y de esta forma mejorar la calidad de la diligencia de indicadores de violencia de género, prestando especial atención a los siguientes indicadores y escenarios de riesgo:*

- *Interésese por conocer si se ha producido algún episodio de violencia física, incluso sin lesión. Por favor, preste especial atención a si la víctima pudo sufrir alguna agresión en la zona del cuello.*
- *Interésese por conocer si se han empleado armas con el objetivo de agredir o amenazar a la víctima y en su caso, el tipo de arma empleada. Respecto a las amenazas, de haberse verbalizado, ¿se trata de amenazas de muerte y/o de suicidio?*
- *Observe si las manifestaciones y/o verbalizaciones espontáneas realizadas tanto por la víctima como por el presunto agresor, u otras fuentes de información, llevan a pensar que no se trata de un episodio aislado, sino reiterado, conllevando un cierto incremento de la violencia o cronificación de esta.*
- *Preste atención a si, con la información disponible en el lugar de actuación, parece que los hechos actuales u otros previos pueden estar motivados total o parcialmente por los celos del presunto agresor.*
- *Observe si de las manifestaciones u otras informaciones se desprende la existencia de algún tipo de conducta de control y/o acoso por el presunto agresor, de su entorno, así como del contexto familiar de la víctima.*
- *Preste atención a si durante esta, u otra intervención policial previa, se han registrado faltas de respeto o conductas desafiantes hacia el personal policial actuante por parte del presunto agresor. Por otra parte, observe también si existen daños en el lugar de los hechos provocados por el presunto agresor.*
- *Observe e interésese por conocer y si el presunto agresor presenta algún trastorno mental y/o suele ser muy impulsivo o agresivo con alteraciones del comportamiento, añadiendo especialmente si existen o han existido ideas o tentativas de suicidio, así como también una posible adicción o abuso de tóxicos, incluido el alcohol.*
- *Observe y preste atención a las manifestaciones y/o verbalizaciones espontáneas realizadas por la víctima para conocer si esta presenta algún de discapacidad, cuadros depresivos u otros trastornos mentales, especialmente si expresa ideas o tentativas de suicidio, así como también una posible adicción o abuso de tóxicos. Solicite, si es posible e indicado, alguna explicación adicional al respecto para canalizar algún tipo de ayuda.*
- *Interésese por conocer si de la información obtenida durante la actuación se deduce que la víctima ha*

expresado al agresor su intención de romper la relación recientemente.

- *Observe e interésese por conocer si de su observación o de las manifestaciones de la víctima o terceras personas se deduce que la víctima piensa que el agresor es capaz de agredirla con mucha violencia o incluso matarla.*
- *Constate la posible existencia de menores a cargo de la víctima y, en su caso, preste atención a si hay algún elemento que indique que estos han sufrido amenazas a la integridad física por parte del presunto agresor, y/o la víctima teme por su seguridad. "*

Queda acreditado que no existe mención alguna relativa a los derechos de protección de datos personales de las víctimas de violencia de género, ni en el citado protocolo de actuación ni en el anexo del mismo.

TERCERO. La parte reclamada aportó asimismo durante las actuaciones de investigación "*Guía de derechos para las mujeres víctimas de violencia de género.* Queda acreditado que dentro de dicha guía se encuentra un apartado relativo a "*Derechos de las víctimas del delito de los que también son titulares las víctimas de violencia de género"* con los siguientes subapartados:

- "4*. Derechos de las víctimas del delito de los que también son titulares las víctimas de violencia de género*

  - *4.1. Derechos del Estatuto de la víctima del delito*
  - *4.2. Derecho a formular denuncia*
  - *4.3. Derecho a solicitar una orden de protección.*
  - *4.4. Derecho a solicitar una orden europea de protección*
  - *4.5. Derecho a ser parte en el procedimiento penal: el ofrecimiento de acciones*
  - *4.6. Derecho a la restitución de la cosa, reparación del daño e indemnización del perjuicio causado*
  - *4.7. Derecho a recibir información sobre las actuaciones judiciales*
  - *4.8. Derecho a la protección de la dignidad e intimidad de la víctima en el marco de los procesos relacionados con la violencia de género*
  - *4.9. Ayudas a las víctimas de delitos considerados violencia de género"*

Dentro del subapartado "*Derecho a la protección de la dignidad e intimidad de la víctima en el marco de los procesos relacionados con la violencia de género"* se encuentra el siguiente contenido:

- *“La Ley Orgánica 1/2004 prevé medidas específicas de protección de la dignidad e intimidad de la víctima. Por un lado, se establece que los datos personales de la misma, de sus descendientes y las personas que estén bajo su guarda o custodia, tengan carácter reservado.*

- *La reserva del nuevo domicilio, centro de trabajo o colegios de los hijos no sólo preservan la intimidad de la víctima sino que, además, es un instrumento importante para su seguridad, al evitar que estos datos puedan llegar a conocimiento del imputado. Con esta misma finalidad, el modelo de solicitud de la orden de protección dispone que la víctima puede indicar un domicilio o teléfono de una tercera persona a la que las Fuerzas y Cuerpos de Seguridad o los órganos judiciales podrán hacer llegar las comunicaciones o notificaciones.*

- *Por otra parte, la Ley del Estatuto de la víctima del delito reconoce el derecho de las víctimas a la protección de su intimidad en el marco del proceso penal, y en este sentido, obliga a jueces, fiscales, funcionarios encargados de la investigación y cualquier persona que de cualquier modo intervenga o participe en el proceso, a adoptar las medidas necesarias para proteger la intimidad de las víctimas y de sus familiares, de acuerdo con lo dispuesto en la Ley. En particular, respecto de las víctimas menores de edad o de víctimas con discapacidad necesitadas de especial protección, deberán adoptar las medidas para impedir la difusión de cualquier tipo de información que pueda facilitar su identificación.*

- *A este respecto, según la Ley de Enjuiciamiento Criminal, el Juez podrá acordar, de oficio o a instancia del Ministerio Fiscal o de la víctima, la adopción de cualquiera de las medidas siguientes cuando resulte necesario para proteger la intimidad de la víctima o el respeto debido a la misma o a su familia:*

- *Prohibir la divulgación o publicación de información relativa a la identidad de la víctima, de datos que puedan facilitar su identificación de forma directa o indirecta, o de aquellas circunstancias personales que hubieran sido valoradas para resolver sobre sus necesidades de protección. Prohibir la obtención, divulgación o publicación de imágenes de la víctima o de sus familiares. Asimismo, el Juzgado puede acordar, de oficio o a instancia de la propia víctima o del Ministerio Fiscal, que las actuaciones judiciales no sean públicas y que las vistas se celebren a puerta cerrada.”*

Se constata que, en la mencionada guía, incluido dicho subapartado, no se encuentra referencia alguna a la normativa general (RGPD o LOPDGDD) o específica en materia de protección de datos personales (LO 7/2021), ni a los derechos derivados de la misma.

CUARTO. En el expediente administrativo del presente procedimiento consta la presentación por la parte reclamada de dos documentos consistentes en las diligencias de derechos Dirección General de la Policía y de la Guardia Civil, los cuales son incorporados posteriormente al correspondiente atestado y a través de los cuales se informa a la víctima de violencia de género de los derechos que le asisten.

Así, por lo que se refiere a la Diligencia de Derechos de la Dirección General de la Policía se encuentran enunciados diversos derechos, divididos en los siguientes apartados:

- *Derecho a la información*
- *Derecho a la asistencia jurídica gratuita*
- *Derecho a la asistencia social integrada*
- *Derecho a la protección de su persona*
- *Derechos laborales y de seguridad social*
- *Derecho a la percepción de ayudas sociales*
- *Acceso a la vivienda y residencia públicas para mayores*
- *Derechos de la víctima extranjera reagrupada o en situación irregular*

Dentro del contenido de dichos apartados no se encuentra referencia alguna a la normativa en materia de protección de datos, ni tampoco de los derechos garantizados derivados de la misma.

Por lo que se refiere a la Diligencia de Derechos de la Guardia Civil, se constata el siguiente contenido relativo a los derechos que le asisten:

- *"A estar acompañada de una persona de su elección desde el primer contacto con las autoridades y funcionarios.*
- *A denunciar, y obtener una copia de la denuncia, debidamente certificada, y en su caso el procedimiento para interponer la denuncia y derecho a facilitar elementos de prueba las autoridades encargadas de la investigación*
- *A la asistencia lingüística gratuita y a la traducción escrita de la copia de la denuncia presentada cuando no entienda o no hable ninguna de las lenguas que tenga carácter oficial en el lugar en el que se presenta la denuncia. Excepcionalmente la traducción escrita de la denuncia podrá sustituirse por un resumen oral de su contenido.*
- *A una vez personada en la causa, tomar conocimiento de lo actuado e instar lo que es su derecho convenga.*

- *A conocer el procedimiento para obtener asesoramiento y defensa jurídica y, en su caso, condiciones en las que puede obtenerse gratuitamente.*
- *A mostrarse parte en el proceso mediante nombramiento de Abogado y Procurador o que le sea nombrado de oficio en caso de ser titular del derecho a asistencia jurídica gratuita según la ley 1/1996 y RD 2103/1996 y ejercitar las acciones civiles y penales que procedan o solamente unas u otras según le convenga. Este derecho deberá ejercitarse antes de la apertura de juicio oral.*
- *A renunciar a la restitución de la cosa reparación del daño e indemnización del perjuicio causado."*

Dentro del contenido de dichas diligencias, se constata la inexistencia de información relativa a los derechos que le asisten en materia de protección de datos, así como a la normativa donde se encuentran los mismos.

QUINTO: De la documentación aportada durante el transcurso del presente procedimiento se desprende, en el momento del inicio de las actuaciones de investigación, la ausencia de la Evaluación de Impacto de Datos Personales (EIPD) prevista en el artículo 35 respecto al tratamiento realizado por el sistema VioGén. Durante las actuaciones de investigación se aportó por la parte reclamada información relativa a la decisión de la realización de una EIPD, cuando en junio del año 2021, se adaptó el tratamiento conforme a la normativa en ese instante en vigor. Según la documentación aportada por la parte reclamada se llega a la conclusión de que no es necesario la realización de una EIPD por no tratarse un sistema ni concurrir las circunstancias de la LO 7/2021:

"En ese entorno factico y legal, no se consideró la necesidad de realizar una EIPD dado que no se trataba de un sistema nuevo o que concurrieran las circunstancias del artículo 35 de la LOPDP"

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 49 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 (en lo sucesivo, LO 7/2021), atribuye a las autoridades de protección de datos, conforme a lo establecido en el artículo 48 de la citada LO 7/2021 y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos

Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

Por último, el artículo 52 *"Régimen aplicable a los procedimientos tramitados ante las autoridades de protección de datos"* de la LO 7/2021 establece que:
"1. En el caso de que los interesados aprecien que el tratamiento de los datos personales haya infringido las disposiciones de esta Ley Orgánica o no haya sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 21, 22 y 23 tendrán derecho a presentar una reclamación ante la autoridad de protección de datos.
2. Dichas reclamaciones serán tramitadas por la autoridad de protección de datos competente con sujeción al procedimiento establecido en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, a la legislación de las Comunidades Autónomas que resulte de aplicación. Tendrán carácter subsidiario las normas generales sobre los procedimientos administrativos y el régimen jurídico del sector público."

II
Régimen jurídico aplicable

El 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 al determinar su ámbito de aplicación material establece en su artículo 2 una serie de tratamientos de datos personales en las que el mismo no resulta aplicable. Entre dichos tratamientos se encuentra en el apartado d) el ejercido *“por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención”.*

Para tratamientos de dicha naturaleza resulta de aplicación la vigente Ley Orgánica 7/2021, de 26 de mayo, a través de la cual se transpone a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del parlamento europeo y del consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o

enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

En este sentido, dicha ley orgánica tiene como objeto, según su artículo primero, *"establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública."*

Asimismo, el artículo segundo, al delimitar su ámbito de aplicación establece que dicha norma será de aplicación *"al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública."*

Por su parte, el artículo 61 de la citada LO 7/2021 establece que el ejercicio de la potestad sancionadora que corresponde a las autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en cuanto no la contradiga, con carácter supletorio, por la normativa sobre el procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público.

III
Contestación a las alegaciones presentadas frente al acuerdo de inicio

El artículo 88 de la LPACAP establece que "La resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo."

En consonancia con el contenido de dicho precepto, si bien no han sido presentadas alegaciones frente a la propuesta de resolución dictada por el instructor del presente procedimiento, resulta oportuno hacer referencia en esta resolución a las alegaciones presentadas por la interesada frente a dicho acuerdo de iniciación. De esta forma, se garantiza la debida separación entre la fase instructora y sancionadora que se prevé por el artículo 63 de la LPACAP como especialidad para los procedimientos de naturaleza sancionadora.

Del mencionado escrito de alegaciones presentado frente al acuerdo de inicio del presente procedimiento, destacaba lo siguiente:

- En relación con la infracción prevista en el artículo 58 apartado f) de la LO 7/2021, consistente en omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal, negaba una ausencia total de información a las personas interesadas en materia de protección de datos, afirmando cumplir con la obligación de informar a las personas cuyos datos personales vayan a ser tratados. Sostiene que, dentro de las actuaciones que se derivan de atribución a una persona de una conducta constitutiva de delito de violencia de género, se generan diversos tratamientos de datos con distintos responsables. Asimismo, se alega que en las diligencias de comunicación a la víctima del nivel de riesgo y en el plan de protección aplicable ya se recoge información relativa al Sistema VioGén.

- Respecto a la infracción consistente en no haber realizado la evaluación de impacto prevista en el artículo 35 Ley 7/2021, alega haber mantenido una actitud proactiva más allá de la de rellenar el documento formal de evaluación de impacto exigido. Además, se afirma que las actuaciones similares de protección ya fueron tenidas en cuenta antes de la entrada en vigor de la ley, no habiendo sido objeto de ningún procedimiento sancionador por parte de la agencia. Por último, sostiene que el mencionado artículo 35 exige que la evaluación debe realizarse con carácter previo al tratamiento y no una vez el mismo está desarrollado pues, en caso contrario, se podrían generar conductas que vulnerarían los derechos de las personas.

Antes de abordar la contestación a las citadas alegaciones, de igual forma que realizó el instructor en la propuesta de resolución, conviene hacer especial referencia a la naturaleza del cargo de la persona que redactó y firmó el mencionado escrito de alegaciones. Tal y como consta en el expediente administrativo del presente procedimiento, las alegaciones fueron elaboradas y firmadas electrónicamente por el Delegado de Protección de Datos designado para la Secretaría de Estado de Seguridad y no por el responsable del tratamiento. A tal respecto, conviene señalar, aunque sea de forma sucinta, las distintas funciones y roles que la Ley 7/2021 atribuyen a ambas figuras, norma la cual resulta de aplicación en el presente supuesto.

Así, el artículo 5 de la mencionada norma define al 'responsable del tratamiento' como "*la autoridad competente que, sola o conjuntamente con otras, determina los fines y medios del tratamiento de datos personales. En caso de que los fines y medios estén determinados por el Derecho de la Unión Europea o la legislación española, estas normas pueden designar al responsable del tratamiento o establecer los criterios para su nombramiento.*"

Por su parte, la figura del Delegado de Protección de Datos (en adelante DPD) se encuentra regulada en la sección tercera del Capítulo IV de la ley y su existencia resulta necesaria, tal y como establece el artículo 40, salvo que se trate de órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales. La exposición de motivos define a esta figura como el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos.

Entre las funciones del mismo, enunciadas en el artículo 42, destaca la de informar y asesorar al responsable y a los empleados sobre las obligaciones, supervisar el cumplimiento de la Ley Orgánica y de otras disposiciones de Protección de Datos, así como cooperar con las Autoridades de Protección de Datos. La naturaleza del DPD implica una especial autonomía e independencia respecto del responsable del tratamiento, tal y como establece el artículo 41 según el cual "*se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses.*"

Por otro lado, en lo que se refiere concretamente a la interposición de alegaciones en un procedimiento sancionador, debe tenerse en cuenta que tal y como dispone el artículo 6 de la mencionada ley, es el responsable del tratamiento quien debe garantizar y demostrar el cumplimiento de las obligaciones exigidas por el artículo.

Teniendo en cuenta los citados preceptos, debe ser el responsable del tratamiento quien, en caso del presente procedimiento sancionador, presente las alegaciones que estime oportunas frente al acuerdo de iniciación con el fin de acreditar su cumplimiento con la normativa. Por el contrario, la presentación de dichas alegaciones por parte del DPD, como se indica en la propuesta, conlleva la existencia de un conflicto de intereses, dado que afecta a la especial autonomía e independencia a la que se ha hecho referencia anteriormente. Si el DPD asume la defensa del responsable en un procedimiento sancionador, su independencia se ve comprometida, pues en tal caso se está actuando en interés del responsable y no en su rol neutral de supervisión.

En este sentido, permitir o atribuir a un DPD la defensa de procedimientos sancionadores en materia de protección de datos implica una interferencia en las funciones del aquel, hecho que se encuentra calificado como infracción grave en el artículo 59 de la ley 7/2021 el cuál fue incorporado por el instructor en la propuesta y que asimismo, se confirma en la presente resolución en los términos que mas abajo se exponen.

Alegación frente a la infracción del artículo 58 f) de la Ley 7/2021. Respecto a la infracción prevista en el artículo 58 apartado f) de la Ley 7/2021, consistente en omisión del deber de informar al interesado acerca del tratamiento de sus

datos de carácter personal, se niega una ausencia total de información a las personas interesadas en materia de protección de datos, afirmando haber cumplido con la obligación de informar a las personas cuyos datos personales vayan a ser tratados. Se indica que dentro de las actuaciones que se derivan de atribución a una persona de una conducta constitutiva de delito de violencia de género, se generan diversos tratamientos de datos con distintos responsables como las Autoridades Judicial del Orden Penal y el Ministerio Fiscal, los cuerpos policiales actuantes y el que se efectúa en el Sistema VioGen. Asimismo señala que en las diligencias de comunicación a la víctima del nivel de riesgo y del plan de protección aplicable se recoge información relativa al Sistema Viogen.

De dicha afirmación se desprende la existencia de diversos tratamientos de datos dentro del ciclo de actuaciones que se derivan de la atribución a una persona de una conducta constitutiva de delito de violencia de género. A tal respecto, conviene indicar que cada uno de dichos tratamientos, aun relacionados entre sí en el marco de la investigación y el proceso judicial, resultan independientes y diferenciados a efectos de su sujeción a la normativa de protección de datos. Ello supone que la obligación de informar sobre el tratamiento de datos con el contenido exigido por el artículo 21, debe aplicarse de manera individual a cada uno de dichos tratamientos y, en consecuencia, corresponde a cada uno de los responsables facilitar la información exigida por la normativa respecto al tratamiento que pretende realizar.

En este sentido, cobra especial relevancia la reciente sentencia de 11 de enero de 2024 del Tribunal de Justicia de la Unión Europea (C-231-22) que define y desarrolla los supuestos en los que existe una cadena de tratamiento de datos. Dicha sentencia, destaca en estos casos la continuidad y la interconexión entre los distintos agentes involucrados en el tratamiento de los mismos datos personales bajo un marco legal común. Este enfoque es de gran utilidad para el análisis del tratamiento de datos personales realizado a través de los formularios del sistema VioGén y los procesamientos judiciales subsiguientes.

En el contexto del sistema VioGén y la actuación de jueces y tribunales, se establece una cadena de tratamiento de datos personales donde cada eslabón (representado por diferentes agentes como, los cuerpos policiales, los servicios de asistencia a las víctimas, y el sistema judicial) procesa los datos con fines específicos que, aunque diferenciados, están intrínsecamente conectados por un objetivo común: proteger a las víctimas y llevar a cabo el procedimiento adecuado frente a los hechos delictivos. La determinación de los fines y medios de estos tratamientos de datos, aunque realizada por agentes distintos, se enmarca dentro de un conjunto de disposiciones legales que definen y regulan sus actividades. Ello implica que, aunque no haya un acuerdo directo entre estos agentes sobre los objetivos y métodos específicos del tratamiento de datos, la normativa nacional establece de manera implícita una red de obligaciones y responsabilidades que unen los diferentes tratamientos.

El mencionado marco legal, que regula la cadena de tratamiento de datos personales, asegura que cada agente cumpla con sus responsabilidades en materia de protección de datos, garantizando los derechos de las víctimas en cada etapa del proceso. Ello incluye el derecho a ser informado sobre cómo y por quién se tratan sus datos personales, el derecho a acceder a sus datos, y el derecho a solicitar la rectificación o supresión de los mismos, entre otros.

Por tanto, la cadena de tratamiento de datos en relación con las actuaciones en materia de violencia de género en el caso de VioGén se caracteriza por la sucesión de tratamientos de datos personales que, aunque realizados por agentes diferentes, están unidos por fines legales claramente definidos y por obligaciones que, aunque distribuidas entre los distintos eslabones de la cadena, forman un sistema coherente que tiene como fin proteger los derechos de las personas

En conclusión, el enfoque de cadena de tratamiento implica una coordinación funcional entre los diferentes agentes, donde la normativa nacional actúa como un elemento unificador que establece tanto los fines compartidos como las responsabilidades específicas de cada agente dentro de la cadena, asegurando, de esta forma una protección efectiva de los datos personales y de los derechos de las personas implicadas a lo largo de todo el proceso.

En el presente supuesto, tal y como resulta de los hechos probados segundo, tercero y cuarto, en lo que se refiere al tratamiento relación realizado por SESDGCE a través del sistema VioGén, se ha constatado el incumplimiento de la obligación de información con con el contenido exigido por el artículo 21 de la LO 7/2021. Tanto en las diligencias de derechos de la Policía Nacional y de la Guardia Civil, en la Guía de derechos de las Víctimas de Violencia, como en los protocolos de actuación, si bien figura normativa y derechos de diversa índole, no existe referencia alguna a los derechos que le asisten en materia de protección de datos personales respecto al tratamiento de aquellos que son recogidos o tratados por el sistema, hecho en base al cual, entre otros motivos, se inició el presente procedimiento sancionador.

En este sentido, el artículo 21 de la LO 7/2021 contempla información que debe de ponerse a disposición de los interesados como la identificación del responsable del tratamiento, los datos de contacto del delegado de protección de datos, los fines del tratamiento a los que se destinen los datos personales, el derecho a presentar una reclamación ante la autoridad de protección de datos o el derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento. Tal y como queda acreditado en los hecho probados segundo, tercera y cuarto, ninguna de esta información se recoge de forma expresa en las diligencias de derechos de la Policía Nacional y de la Guardia Civil que posteriormente se incorporan a los atestados, ni en el

protocolo de valoración policial del riesgo y gestión de la seguridad de las víctimas de violencia de género, ni en la Guía de derechos; documentos todos ellos aportados por la parte reclamada en el transcurso de las actuaciones de investigación.

Como se indicó anteriormente, si bien se ha comprobado la existencia de cierta información en materia de protección de datos relativa al Sistema VioGén en la web del Ministerio del Interior, como más adelante se expondrá, no resulta posible entender cumplida la obligación de información que exige el artículo 20 de la LO 7/2021 con una mera publicación de dicha información en la página web del responsable del tratamiento. Por el contrario, dicha información debe de ser puesta a disposición a los interesados en el momento en que se vayan a tratar datos personales mediante el sistema VioGén, para la cual debería encontrarse expresamente en las distintas diligencias o formularios expedidos previamente a su utilización. Como resulta de los hechos probados tercero y cuarto, esta circunstancia no concurre en la documentación presentada por la parte reclamada, en la cual ni siquiera figura una indicación del sitio web donde se encuentra dicha información publicada.

Alegaciones frente al artículo 35 de la LO 7/2021 Estas alegaciones hacen referencia al incumplimiento de la evaluación de impacto exigido por el artículo 35 de la mencionada ley. En este sentido se afirma haber mantenido una actitud proactiva más allá de rellenar un documento formal que podría haber denominado evaluación de impacto. Asimismo, se señala que las actuaciones similares de protección ya se tenían en cuenta antes de la entrada en vigor de la ley no habiendo sido objeto de ningún procedimiento sancionador por parte de esta autoridad, habiéndose producido el tratamiento por más de 15 años.

A tal respecto, conviene indicar que el hecho de haber mantenido una actitud proactiva en determinados aspectos en materia de protección de datos no sustituye la necesidad de cumplir con la obligación de realizar una EIPD cuando concurren las circunstancias determinadas por la normativa. La LO 7/2021 establece claramente que, en casos de tratamientos que supongan un alto riesgo para los derechos y libertades de las personas físicas, es obligatorio realizar formalmente una evaluación de impacto detallada con la información exigida por el artículo 35 de la misma norma. Dicha evaluación no se trata de un simple trámite burocrático, sino que supone una herramienta esencial para identificar y mitigar riesgos específicos relacionados con el tratamiento de datos. Asimismo, la realización de la evaluación de impacto es una obligación independiente y no se ve mitigada por el hecho de haber implementado medidas de protección de datos antes de la entrada en vigor de la ley.

Por otro lado, el hecho de que el tratamiento de datos se haya llevado a cabo durante más de 15 años sin sanciones previas de la presente autoridad no exime al responsable de cumplir con las obligaciones actuales. La normativa en materia de protección de datos ha evolucionado significativamente,

especialmente con la entrada en vigor del RGPD y de la aprobación de la Ley 7/2021 y las prácticas anteriores no necesariamente se alinean con los estándares actuales de protección de datos.

Como última alegación se afirma que el mencionado artículo 35 de la LO 7/2021 exige que dicha evaluación debe realizarse con carácter previo al tratamiento y no una vez el mismo está desarrollado ya que, en caso contrario, se podrían generar conductas que pudieran vulnerar los derechos de las personas. A tal respecto, se reitera que el sistema fue creado antes de la entrada en vigor de dicha Ley.

Frente a esta última alegación resulta oportuno destacar que lo que persigue el precepto a través de la exigencia de que dicha evaluación se realice previamente al tratamiento es, precisamente, la evaluación de potenciales situaciones de alto riesgo en los derechos y libertades de los interesados y evitar, en la medida de lo posible, que dichos riesgos se materialicen. Tales riesgos, además, varían con el tiempo, debido a que las circunstancias en las que se producen los tratamientos (contexto, naturaleza, alcance o fines) no permanecen incólumes a lo largo del tiempo. Ello requiere, en consecuencia, una evaluación continua que, por lo que atañe a la EIPD, supone la realización de una actualización periódica a medida que el contexto, naturaleza, alcance o fines del tratamiento (incluyendo la tipología y número de datos personales tratados) van variando a lo largo del tiempo.

Como consecuencia de lo indicado, cada vez que el sistema VioGén procede a tratar datos personales de personas físicas, se produce un nuevo tratamiento de datos del cual resultará de plena aplicación la normativa vigente. Por tanto, aunque el sistema fuera creado antes de la entrada en vigor de la LO 7/2021, los tratamientos de datos realizados a partir de la implementación de la nueva normativa exigen la existencia de la previa evaluación de Impacto para que los mismos sean conformes a esa normativa. Contrariamente a la afirmación por la parte reclamada de que la aplicación de la nueva normativa de protección de datos podría vulnerar los derechos de las personas, su implementación refuerza y amplía estas protecciones. De hecho, resulta crucial para identificar y mitigar cualquier riesgo potencial para los derechos y libertades de las personas físicas que pueda surgir debido a la naturaleza, alcance, contexto o fines del tratamiento de datos personales.

IV
Obligación incumplida del artículo 20.1 LO 7/2021

El artículo 20 de la mencionada LO 7/2021 establece las condiciones generales de ejercicio de los derechos de los interesados en materia de protección de datos, estableciendo en su apartado primero que:

“1. El responsable del tratamiento deberá facilitar al interesado, de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo para todas las personas, incluidas aquellas con discapacidad, toda la información contemplada en el artículo 21, así como la derivada de los artículos 14, 22 a 26 y 39.
Además, el responsable del tratamiento deberá adoptar las medidas necesarias para garantizar al interesado el ejercicio de sus derechos a los que se refieren los artículos 14 y 22 a 26.”

Así, de los hechos probados PRIMERO, SEGUNDO, TERCERO Y CUARTO de la presente resolución se desprende que la entidad investigada no ha cumplido con la obligación de información impuesta por el mencionado artículo 20 de la LO 7/2021 a la hora de tratar datos personales de los interesados en relación con el tratamiento de datos realizados por el sistema VioGén.

Como se indica en el hecho probado PRIMERO, El Sistema VioGén (Sistema de Seguimiento Integral de los Casos de Violencia de Género) es un tratamiento de datos de carácter personal cuyo responsable es la persona titular de la Dirección General de Coordinación y Estudios del Ministerio de Interior, el cual “desarrolla las actividades necesarias para garantizar la seguridad y protección de las víctimas de violencia de género, facilitar el seguimiento de las medidas aplicadas y prevenir actividades delictivas vinculadas a la violencia de género con la finalidad de proteger a dichas víctimas y prevenir infracciones penales sobre las mujeres que se puedan ser sujetos pasivos de tales conductas.”

Resulta indudable que a través de la utilización de dicho sistema se produce un tratamiento de datos personales de las personas interesadas, pues su uso conlleva la obtención de información personal facilitada por éstas a través del uso de formularios que contienen una serie de enunciados predeterminados con determinada información considerada relevante u oportuna para cumplir su fin.

En este sentido, el artículo 5 del mismo texto legal define al 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”*

Por su parte, tal y como consta en el hecho probado primero, el Registro de actividades de tratamiento del Ministerio del Interior, cuya última actualización es de fecha 29/09/2023, establece como responsable del tratamiento del Sistema VioGén a la Secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios. (SESDGCE)

Conviene señalar que el tratamiento de los datos personales que se realiza a través de los formularios del sistema VioGén resulta independiente del que, de forma simultánea, anterior o posterior, puedan realizar los jueces y tribunales con el fin de la averiguación, investigación, procesamiento y enjuiciamiento de los presuntos hechos delictivos. Supone, por tanto, dos tratamientos diferenciados, y en ambos debe de garantizarse los derechos en materia de protección de datos de las víctimas, incluido el derecho a ser informado del tratamiento de sus datos personales.

Resulta destacable, asimismo, el hecho de que entre la información a la que se refiere dichos formularios se encuentre la relativa a la salud o la vida sexual de las personas interesadas, los cuales suponen categorías de datos especiales de los previstos en el artículo 13 LO 7/2021, según el cual:

"1. El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:
a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.
b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.
c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos."

No puede obviarse, además, la previsión establecida en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, cuyo artículo 63, relativo a la protección de datos relacionados con la violencia de género establece:

"1. En las actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia."

De la misma forma, el artículo 50 de la reciente Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual establece que *"En las actuaciones y procedimientos relacionados con la violencia sexual se protegerá la intimidad de las víctimas, y en especial sus datos personales."*

En los términos indicados por el hecho probado PRIMERO, se ha podido comprobar la existencia de cierta información en materia de protección de

datos personales, en página web del Ministerio del interior, la cual es desarrollada en el registro de actividades que se encuentra en dicha página. Sin embargo, tal y como resulta de los hechos probados SEGUNDO y TERCERO, no existe referencia alguna relativa a información en materia de protección de datos personales, ni en los protocolos ni en sus anexos, ni en las diligencias de derechos aportadas en el curso de las actuaciones de investigación por dicha entidad.

Debe de tenerse en cuenta que dicha información resulta esencial para garantizar los derechos de las personas interesadas en materia de protección de datos personales, dado que, entre dicha información se encuentra, entre otras, la relativa a la identificación del responsable del tratamiento, la identificación del Delegado de Protección de datos o los fines del tratamiento, información que le va a permitir el ejercicio de los derechos garantizados por la normativa en dicha materia.

Además, en el caso que nos ocupa, el tratamiento de los datos se realiza en un contexto donde las víctimas se encuentran en una situación de especial vulnerabilidad lo que implica que el otorgamiento de la información resulte crucial para garantizar que las mismas tengan pleno conocimiento de los fines del tratamiento de los datos personales que va a facilitar a partir de dicho momento. Ello se muestra en coherencia, no solo con la normativa en materia de protección de datos personales, sino con el espíritu y finalidad de las normas destinadas a la protección de las víctimas de violencia de género.

En este sentido, la mencionada situación de especial vulnerabilidad en que se encuentran las victimas conlleva una mayor exigencia en el cumplimiento de la obligación de información en materia de protección de datos. En base a dicha exigencia, para que resulte efectivo dicho cumplimiento, la información debe ser comunicada de manera clara, accesible y directa en el momento en que se vaya a realizar el tratamiento, Una publicación genérica en una página web, si bien puede resultar útil como medida complementaria, no sustituye la necesidad de comunicarla de manera directa y en el momento pertinente con el fin de que la misma resulte plenamente efectiva y cumpla, de esta forma, con las exigencias previstas por la normativa.

En el caso que nos ocupa, la ausencia de esta información en materia de protección de datos de forma directa y previa a las víctimas cuyos datos van a ser tratados conlleva un incumplimiento del deber de información previsto en el ya mencionado artículo 20 de la misma norma. Debe subrayarse, además, que la obligación de informar cobra una especial relevancia en el presente supuesto teniendo en cuenta la naturaleza del tratamiento, en los que además de afectar a personas en situación de especial vulnerabilidad, entre los datos objeto del tratamiento se encuentran determinadas categorías de datos especiales como ocurre con la salud o la vida sexual de las víctimas.

Por último, cabe hacer una breve alusión al artículo 26 LO 7/2021 al que hace referencia la parte investigada, a tenor del cual *“El ejercicio de los derechos de*

información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales."

A tal respecto, conviene señalar que no existe previsión alguna en la vigente Ley de Enjuiciamiento Criminal relativa al tratamiento de los datos personales. Sí que existe, por el contrario, una referencia expresa en el apartado segundo del artículo 236 ter de la Ley Orgánica 6/1985 del Poder Judicial , el cual establece que *"En el ámbito de la jurisdicción penal, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos, diligencias o expedientes de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal"*

De la misma forma, el artículo 236 *septies* de la misma norma establece, en relación con el tratamiento de los datos personales con fines jurisdiccionales, que *"los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados."*

Por tanto, a falta de previsión expresa en la ley procesal penal, el tratamiento de los datos personales en todas las fases del procesamiento y enjuiciamiento penal, incluida la investigación, así como los derechos de información, acceso, rectificación, supresión, oposición y limitación de los interesados durante el mismo, se rigen por la vigente Ley Orgánica 7/2021, cuyo articulado resulta plenamente aplicable en el presente supuesto.

V
Tipificación y calificación de la infracción

La LO 7/2021 contempla un cuadro de infracciones y sanciones en el caso de incumplimiento de las obligaciones previstas en su articulado, clasificándola en leves, graves y muy graves.

El artículo 58, apartado f) califica como infracción muy grave, "*La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en esta Ley Orgánica."*

De conformidad con las evidencias derivadas del presente procedimiento, se considera que la **SECRETARÍA DE ESTADO DE SEGURIDAD, DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS, DEL MINISTERIO DEL INTERIOR** con **NIF** S2816001H**,** ha cometido la infracción prevista en el artículo 58, apartado f), al no cumplir la obligación de información de las personas interesadas del tratamiento de sus datos de carácter personal que se realiza a través del Sistema de Seguimiento Integral de los casos de Violencia de Género (Sistema VioGén).

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 63 LO 7/2021, que determina dicho plazo para aquellas infracciones tipificadas como muy graves, como ocurre en el presente caso.

VI
Obligación incumplida del artículo 35 LO 7/2021

El artículo 35 LO 7/2021 establece aquellos supuestos en los que resulta necesario la realización, por parte del responsable del tratamiento y con carácter previo, de una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.
2. La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con esta Ley Orgánica. Esta evaluación tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas.
3. Las autoridades de protección de datos podrán establecer una lista de tratamientos que estén sujetos a la realización de una evaluación de impacto con arreglo a lo dispuesto en el apartado anterior y, del mismo modo, podrán establecer una lista de tratamientos que no estén sujetos a esta obligación. Ambas listas tendrán un carácter meramente orientativo."

Con relación a dicha obligación, durante el transcurso de las actuaciones investigadoras y tal y como se indica en el hecho probado QUINTO, la entidad investigada afirmó que, una vez entró en vigor la nueva ley orgánica, se procedió a valorar la pertinencia de dicha evaluación. A tales efectos, se aporta

una tabla donde se analiza el riesgo a la hora de decidir la realización de una Evaluación de Impacto de Datos Personales (EIDP), y en la cual no se consideró necesario realizarla, dado que, afirman, no se trataba de un sistema nuevo ni tampoco concurrían las circunstancias indicadas en el artículo 35 de la LO 7/2021.

En este sentido, para determinar si concurrían las circunstancias previstas del artículo 35 para realizar una EIDP, resulta necesario verificar si en el caso del tratamiento a través del sistema VioGén existía una probabilidad de alto riesgo de los derechos y libertades de las personas físicas, en los términos indicados por el mencionado artículo.

A tal respecto, conviene destacar la naturaleza y fines del tratamiento de los datos personales realizado por parte del sistema VioGén, el cual persigue precisamente una evaluación del riesgo en los derechos y libertades de las víctimas al fin de adoptar las medidas más adecuadas en virtud del nivel de riesgo resultante, tal y como resulta de las actuaciones previas y afirma la propia parte investigada.

En el caso que nos ocupa, la naturaleza de dicho tratamiento manifiesta claramente un alto riesgo para los derechos y libertades de las interesadas, puesto que un tratamiento inadecuado podría poner incluso en riesgo la integridad física y moral de las victimas (piénsese en el posible conocimiento de tales datos por parte del agresor), con el añadido de la existencia de categorías especiales de datos personales en el mencionado tratamiento.

Teniendo en cuenta tales circunstancias, se desprende que, en el presente supuesto, concurrían (y concurren) las condiciones exigidas por el articulo 35 para considerar necesario realizar una EIDP. Dicha evaluación tendrá como fin determinar los riesgos para los derechos y libertades de las víctimas, las medidas para hacer frente a los mismos, así como las medidas de seguridad y mecanismos para garantizar la protección de los datos personales y poder, de esta forma, demostrar su conformidad con la Ley Orgánica.

Por lo que se refiere a la afirmación de la entidad investigada respecto a que no se trataba de un sistema nuevo, conviene señalar que tal circunstancia no exime del cumplimiento de la obligación prevista, una vez la norma desplegó plenos efectos tras su entrada en vigor. Si bien es cierto que la anterior normativa no contemplaba dicha obligación, no es menos cierto que, una vez vigente la nueva ley orgánica, la misma posee plena eficacia. En consecuencia, la nueva obligación deberá aplicarse mediante una evaluación de todos los sistemas creados con anterioridad a su entrada en vigor cuyo tratamiento reúna las condiciones exigidas por el artículo 35, no existiendo en la norma, además, disposición transitoria alguna en este sentido.

Prueba de la vigencia de dicha obligación deriva de la propia actuación de la entidad investigada, la cual procedió a valorar si concurrían o no los requisitos para realizar la evaluación de impacto exigida por la nueva norma y cuyo resultado final fue no realizarla; decisión que, teniendo en cuenta la naturaleza del tratamiento, devino desacertada, a juicio de la presente autoridad.

Conviene, por último, hacer referencia a la previsión que establece el ya mencionado Registro de Actividades de Tratamiento del Ministerio de Interior respecto a las medidas de seguridad y organizativas del sistema Viógen. Dicho Registro establece que *"Las medidas de seguridad implantadas se corresponden con las previstas en el exo II (medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la política de protección de datos y seguridad de la información del Ministerio del Interior y de la Secretaría de Estado de Seguridad."*

A tal respecto, conviene indicar que la mencionada norma que regula el Esquema Nacional de Seguridad tiene un objeto distinto al que corresponde a la normativa de protección de datos. Así, el artículo primero de dicho Real Decreto establece que el citado esquema *"está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias* "

De hecho, el artículo segundo del mencionado Real decreto realiza una remisión expresa a la normativa de protección de datos personales cuando el sistema de información trate datos de dicha naturaleza:

"Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el 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 (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, 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, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

Como puede observarse, en el caso que nos ocupa, en materia de seguridad de protección de datos personales resulta plenamente aplicable la normativa en materia de protección de datos y, en particular, dada la naturaleza del tratamiento, la ya mencionada Ley Orgánica 7/2021, de 26 de mayo, no pudiendo limitarse la adopción de medidas de seguridad al cumplimiento exclusivamente de las normas relativas al Esquema Nacional de Seguridad.

VII
Tipificación y calificación de la infracción

Por tanto, en el presente supuesto nos encontramos ante el incumplimiento de la obligación prevista en el artículo 35 de la LO 7/2021, por parte de la **SECRETARÍA DE ESTADO DE SEGURIDAD, DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS, DEL MINISTERIO DEL INTERIOR** con **NIF** S2816001H al no proceder a la realización de una evaluación de impacto respecto al tratamiento realizado a través del sistema VioGén.

Dicho incumplimiento es calificado como infracción grave por el artículo 59.1 l), LO 7/2021 según el cual *"El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados."*

En este sentido, en el presente supuesto concurren los presupuestos previstos en el tipo infractor dado que, en los términos mencionados anteriormente, se incumplió la obligación de realizar una evaluación de impacto en la protección de los datos de carácter personal de las personas interesadas a pesar de concurrir las circunstancias exigidas por el artículo 35, lo cual implicaba, dada la naturaleza del tratamiento del sistema así como de los datos personales, un riesgo grave para dichas personas.

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los dos años, conforme al artículo 63 LO 7/2021, que determina dicho plazo para aquellas infracciones tipificadas como graves, como ocurre en el presente caso.

VIII
Obligación incumplida del artículo 41 de la LO 7/2021

El artículo 41 de la LO 7/2021 reconoce la especial autonomía e independencia de figura del delegado de protección de datos con el fin de garantizar que realice correctamente sus funciones sin ningún tipo de injerencia, haciendo expresa referencia a evitar cualquier conflicto de intereses:

"El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que

incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses".

Dicho rasgo de independencia deriva de las funciones atribuidas a la mencionada figura y que, como mínimo, debe encomendarle el responsable de tratamiento, las cuales son enumeradas por el artículo 42 de la misma norma:

"El responsable del tratamiento encomendará al delegado de protección de datos, al menos, las siguientes funciones:

a) Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en virtud de esta Ley Orgánica y de otras disposiciones de protección de datos aplicables.

b) Supervisar el cumplimiento de lo dispuesto en esta Ley Orgánica y en otras disposiciones de protección de datos aplicables, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

d) Cooperar con la autoridad de protección de datos en los términos de la legislación vigente.

e) Actuar como punto de contacto de la autoridad de protección de datos para las cuestiones relacionadas con el tratamiento, incluida la consulta previa referida en el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto".

De la lectura de dicho artículo se desprende que dicha enumeración no es exhaustiva, sino que, por el contrario, resulta posible la atribución de otro tipo de funciones distintas que estén relacionadas con la función supervisora y de asesoramiento. Sin embargo, resulta coherente con su naturaleza que la atribución de estas funciones no debe afectar a su independencia ni crear un conflicto de intereses. Respecto a esta afirmación, cobra especial relevancia la reciente sentencia del Tribunal de Justicia de la Unión Europea (Sala Sexta) de 9 de febrero de 2023 (X-FAB Dresden GmbH & Co. KG contra FC) que si bien, se pronuncia sobre cuestiones prejudiciales de determinados artículos RGPD respecto a los delegados, resulta aplicable en el presente caso, en cuanto que se pronuncia sobre el otorgamiento de las funciones y los conflictos intereses-

“En segundo término, no es menos cierto que el responsable del tratamiento o su encargado deben velar por que esas otras funciones y cometidos no impliquen un «conflicto de intereses». Habida cuenta del significado de esos términos en el lenguaje corriente, procede considerar que, conforme al objetivo perseguido por el artículo 38, apartado 6, del RGPD, no se puede encomendar al delegado de protección de datos la ejecución de funciones o de cometidos que puedan perjudicar el desempeño de las funciones que ejerce como delegado de protección de datos.”

[…]

La determinación de la existencia de un conflicto de intereses, en el sentido del artículo 38, apartado 6, del RGPD, debe efectuarse caso por caso, sobre la base de una apreciación del conjunto de las circunstancias pertinentes, en particular, de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos.”

En el caso que nos ocupa, tal y como resulta de la documentación obrante en el expediente del presente procedimiento, el presunto conflicto de intereses consiste en el hecho de permitir o atribuir la defensa en un procedimiento sancionador en materia de protección de datos al DPD mediante la formulación y presentación de las alegaciones frente al acuerdo de inicio de dicho procedimiento el cual iba dirigido hacia la organización para la que presta servicios. En dichos términos, con el fin de determinar la existencia o no un conflicto de intereses y siguiendo la sentencia dictada por el TJUE, resulta necesario, analizar el conjunto de las circunstancias pertinentes de dicha situación.

A tal respecto, debemos de recordar en primer lugar que el papel del DPD, como regla general, es supervisar, asesorar e informar sobre las prácticas de protección de datos dentro de la organización, manteniendo una postura neutral e imparcial. De hecho, la exposición de motivos lo define como *“el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos”.* En este sentido, si el DPD asume la defensa de la organización en un procedimiento sancionador, ya sea administrativa o judicialmente, su capacidad para permanecer independiente e imparcial puede quedar comprometida.

Por otro lado, la presentación de alegaciones en defensa de la organización en un procedimiento sancionador en materia de protección de datos puede ser vista como un alineamiento con los intereses de esta, en lugar de mantener una posición centrada precisamente en la supervisión y asesoramiento en dicha materia. En tal caso, podría encontrarse en la posición de tener que revisar y evaluar su propio asesoramiento o las decisiones que previamente había supervisado o aprobado. Esta circunstancia crea un escenario de "juez y

parte", donde el DPD estaría evaluando la adecuación de sus propias acciones o recomendaciones, lo cual resulta en un claro conflicto de intereses.

Asimismo, existe el riesgo de que el DPD, al involucrarse en la defensa de la organización en un determinado procedimiento sancionador, pueda recibir presiones internas por parte del responsable del tratamiento. Dichas presiones pueden influir en sus decisiones, comprometiendo su autonomía y capacidad para actuar en el mejor interés de la protección de datos. De la misma forma, la credibilidad del DPD ante los empleados de la organización y ante terceros (incluidas las propias autoridades de protección de datos) puede verse afectada, lo que erosiona la confianza en su capacidad para desempeñar sus funciones de una manera objetiva e independiente.

Tampoco debe desdeñarse la naturaleza de los datos personales tratados en el presente caso que tienen como fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. La naturaleza de dichas de materias, por su afectación directa a los derechos y libertades, hace aún más necesario la independencia y supervisión del DPD. De hecho, a diferencia de lo que ocurre con el RGPD, en el caso de estas materias la Ley 7/2021 establece como regla general la existencia del DPD como obligatoria, salvo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales, tal y como afirma el artículo 40.

Para finalizar conviene hacer referencia las directrices sobre los delegados de protección de datos adoptadas por el Grupo de Trabajo sobre Protección de Datos del Artículo 29, que si bien también hacen referencia al RGPD, resulta de de utilidad en cuanto a la interpretación y definición de “conflicto de intereses”:

“El artículo 38, apartado 6, permite a los DPD «desempeñar otras funciones y cometidos». No obstante, requiere que la organización garantice que «dichas funciones y cometidos no den lugar a conflicto de intereses».

La ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses.

Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del

departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento.

Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o al encargado del tratamiento ante los tribunales en casos relacionados con la protección de datos".

IX
Tipificación y calificación

El artículo 59, apartado d) califica como muy grave la siguiente infracción:

"d) La falta de designación de un delegado de protección de datos en los términos previstos en el artículo 40 o no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones".

De acuerdo con lo expuesto anteriormente, la atribución de funciones a un Delegado de Protección de Datos (DPD) supone ocasionar un conflicto de intereses, lo cual puede considerarse como una injerencia en sus funciones establecidas, dado su condición de principal o figura de asesoramiento y supervisión de los responsables de protección de datos, como así lo reconoce la Ley 7/2021.

Dicha interferencia tiene lugar en el momento que se le atribuye la tarea de interponer alegaciones ante el presente procedimiento sancionador, dado que se le exige al DPD asumir un rol que se desvía significativamente de sus funciones de supervisión y asesoramiento. La nueva responsabilidad podría interferir con sus deberes primordiales, y mermar la independencia que caracteriza al mismo.

Debe tenerse en cuenta que, tal y como consta en el presente expediente el acuerdo de inicio fue dirigido frente al responsable del tratamiento y no frente al DPD, lo cual excluye cualquier tipo de confusión y/o error entre el dicho responsable y esta autoridad.

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los dos años, conforme al artículo 63 LO 7/2021, que determina dicho plazo para aquellas infracciones tipificadas como graves, como ocurre en el presente caso.

X
Propuesta de sanción

El apartado primero del artículo 62 LO 7/2021 relativo a las sanciones**,** establece que *"En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo."*

El mencionado artículo 77.1 de la Ley Orgánica 3/2018 establece que" El *régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

XI
Adopción de medidas

El artículo 61 de la LO 7/2021 relativo al régimen jurídico del régimen sancionador, establece que el *"ejercicio de la potestad sancionadora que corresponde a las autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en cuanto no la contradiga, con carácter supletorio, por la normativa sobre el procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público."*

Asimismo, el apartado primero del artículo 62 establece que *"En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo"*

En base a dichas disposiciones y teniendo en cuenta que la parte investigada se encuentra entre los sujetos previstos en el artículo 77.1, a través de la presente resolución se acuerda imponer al responsable la adopción de las siguientes medidas correctivas para ajustar su actuación a la normativa en el plazo que seguidamente se indica:

- Incluir, en un plazo máximo de tres meses, la información en materia de protección de datos exigida por el artículo 21 de la LO 7/2021 en todos aquellos documentos y/o diligencias facilitadas a las víctimas en el momento en que se vayan a tratar sus datos personales, de forma que se cumpla de forma efectiva la obligación prevista en el artículo 20 de dicha norma.

- Implementar, en un plazo máximo de tres meses, las medidas necesarias con el fin de garantizar la autonomía e independencia del DPD y evitar, de esta forma, cualquier situación que le origine un conflicto de intereses.

- Proceder, en un plazo máximo de seis meses, la realización y superación de la Evaluación de Impacto de Datos personales en los términos y con el contenido mínimo exigido por el artículo 35 LO 7/2021.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa prevista en el artículo 58 apartado m) de la LO 7/2021, que califica como infracción muy grave: *m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50.*

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

PRIMERO: DECLARAR que **S. DE E. DE SEGURIDAD**, con **NIF** S2816001H ha cometido las siguientes infracciones previstas en la LO 7/2021

- Infracción del artículo 20 de la LO 7/2021, tipificada en el artículo 59 f)
- Infracción del artículo 35 de la LO 7/2021, tipificada en el artículo 59.e)
- Infracción del artículo 41 de la LO 7/2021, tipificada en el artículo 59.l)

SEGUNDO: ORDENAR a S. DE E. DE SEGURIDAD, con **NIF** S2816001H, a que en virtud del artículo 62 de la LO 7/2021, desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las siguientes medidas correctivas en el plazo que seguidamente se indica:

- Incluir, en un plazo máximo de tres meses, la información en materia de protección de datos exigida por el artículo 21 de la LO 7/2021 en todos aquellos documentos y/o diligencias facilitadas a las víctimas en el momento en que se vayan a tratar sus datos personales, de forma que se cumpla de forma efectiva la obligación prevista en el artículo 20 de dicha norma.

- Implementar, en un plazo máximo de tres meses, las medidas necesarias con el fin de garantizar la autonomía e independencia del DPD y evitar, de esta forma, cualquier situación que le origine un conflicto de intereses.

- Proceder, en un plazo máximo de seis meses, a la realización y superación de la Evaluación de Impacto de Datos personales en los términos y con el contenido mínimo exigido por el artículo 35 LO 7/2021.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa prevista en el artículo 58 apartado m) de la LO 7/2021, que califica como infracción muy grave: *m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50*

TERCERO: NOTIFICAR la presente resolución a **S. DE E. DE SEGURIDAD** con **NIF** S2816001H

CUARTO: Comunicar la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD, aplicable en virtud del artículo 62 de la LO 7/2021.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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

siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-16012024

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