- **Procedimiento Nº: PS/00509/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Mediante Acuerdo de fecha 03/01/22, se inició el procedimiento sancionador, PS/0509/2021, instruido por la Agencia Española de Protección de Datos ante la DIRECCIÓN GENERAL DE LA POLICÍA, (DGP), (en adelante, "la parte reclamada"), por presunta infracción del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/16, 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, (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD), y teniendo como base los siguientes:

ANTECEDENTES:

PRIMERO: Con fecha 02/06/21, tuvo entrada en esta Agencia, un escrito de ***A.A.A.,*** (en adelante, "la parte reclamante"), en el cual, entre otras, indicaba lo siguiente:

> *"El pasado día 01/06/21 me encontraba junto a un grupo de amigos en la confluencia de las calles General Aranaz con María Lombillo Madrid. Nos encontrábamos abandonando una concentración que había sido convocada por la asociación "mi barrio seguro" y cuando abandonamos la concentración, varios indicativos del CNP procedieron a identificarnos y pasar nuestros datos por la emisora a los efectos de realizar las oportunas comprobaciones. Una vez finalizado el proceso de identificación y tras comprobar los agentes que todo estaba correcto, el agente procedió a tomar fotografías de nuestros DNI con su teléfono personal, todo ello, a pesar de ser advertido por los presentes de que no otorgábamos nuestro consentimiento para esa toma de fotografías del DNI. La propia agente nos manifestó que las fotografías se estaban tomando desde su teléfono personal, ya que, ellos no tienen teléfono de dotación".*

SEGUNDO: Con fecha 01/07/21, de conformidad con lo estipulado en el artículo 65.4 de la Ley LOPDGDD, por parte de esta Agencia, se dio traslado de dicha reclamación a la DGP, para que procediese a su análisis e informase, en el plazo de un mes, sobre lo que exponía en el escrito de reclamación.

TERCERO: Con fecha 23/07/21, la DGP remite a esta Agencia escrito de contestación a la solicitud hecha, en el cual, entre otras indicaba lo siguiente:

> *"La Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, regula en su artículo 16, los supuestos y la forma en la que los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas, habilitándoles para "realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados", debiendo respetar estrictamente "los principios de proporcionalidad, igualdad de trato y no discriminación por razón de*

nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social".

En este sentido, la norma referida prevé incluso que cuando no fuera posible la identificación por cualquier medio, los agentes podrían "requerir a quienes no pudieran ser identificados a que los acompañen a las dependencias policiales más próximas en las que se disponga de los medios adecuados para la práctica de esta diligencia, a los solos efectos de su identificación y por el tiempo estrictamente necesario.

En un contexto como el actual marcado por la situación de pandemia internacional provocada por el coronavirus COVID-19, la práctica de las diligencias de identificación lleva implícito un incremento de riesgo personal para los actuantes. Por este motivo y de acuerdo con los consejos difundidos por las autoridades sanitarias, los agentes policiales extreman las medidas de autoprotección de los agentes, también en el ámbito de la salud y la higiene, evitando el contacto directo con el identificado y sus pertenencias, buscando condiciones ambientales de asepsia y manteniendo distancias de seguridad.

En este sentido, el único objeto de tomar una imagen del documento de identidad y con ella practicar las comprobaciones oportunas, fue evitar la manipulación de este y mantener la distancia de seguridad. De esta forma, la toma de la fotografía es un modo de proceder excepcional en un momento marcado por circunstancias sanitarias y sociales de grave riesgo para la salud.

A fin de conocer las circunstancias concretas en las que se produjeron los hechos arriba descritos, se evacuó consulta a la Jefatura Superior de Madrid.

Del informe se obtienen las siguientes conclusiones: - Se ha constatado que la funcionaria tomó una sola imagen del Documento Nacional de Identidad de la persona identificada, actuando al amparo del artículo 16 de la LO 4/2015, y con los mismos efectos y finalidad que si hubieren sido tomados los datos de manera manual. - Como consta en su Minuta-Informe, la agente procedió a borrar la imagen del documento una vez cumplida la finalidad para la cual se tomó.

Ha de señalarse que la actuación policial de prevención delictual y mantenimiento del orden público, objeto del presente informe, se acomodó específicamente a los principios básicos de actuación establecidos en el artículo 5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, así como a la legislación vigente en materia de protección de datos, concretamente: • 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, la cual ha sido traspuesta al ordenamiento español mediante: • Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

de Carácter Personal, vigente en el momento de los hechos. • Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la que se recogen las siguientes especificaciones. o Disposición derogatoria única. Derogación normativa. 1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Concretamente, el artículo 2.2 apartado a) de la citada Ley Orgánica 3/2018 en relación al artículo 2.2 apartado d) del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2.016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos expresamente excluye la aplicación de la Ley Orgánica 3/2018 al tratamiento de datos personales "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".

Se participa que, desde la Dirección Adjunta Operativa, se procederá a impartir instrucciones sobre el uso de dispositivos electrónicos por parte de funcionarios policiales en actuaciones operativas, de manera que se asegure la conformidad de dichas actuaciones a la normativa en materia de Protección de Datos".

CUARTO: Con fecha 18/10/21, de conformidad con el artículo 65 de la Ley LPDGDD por parte de la Directora de la Agencia Española de Protección de Datos se dicta acuerdo de admisión de trámite de la reclamación presentada, al apreciar posibles indicios racionales de una vulneración de las normas en el ámbito de las competencias de la Agencia Española de Protección de Datos.

QUINTO: Con fecha 03/01/22, por parte de la Directoria de la Agencia Española de Protección de Datos, se inicia procedimiento sancionador a la DGP, por vulneración del RGPD, al apreciar posibles indicios de infracción del 32.1 del RGPD.

SEXTO: Notificado el acuerdo de inicio a la DGP, ésta mediante escrito de fecha 14/01/22 formuló, en síntesis, las siguientes alegaciones:

"Respecto de la diligencia de identificación, el acuerdo de procedimiento sancionador PS/00509/2021, realiza un análisis de la Ley Orgánica 4/2015 de 30 de marzo, de protección de la seguridad ciudadana (en adelante, LOPSC), haciendo alusión, en primer lugar al preámbulo donde se indica que "…se habilita a las autoridades competentes para acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación…".

También se hace referencia a los artículos 9, sobre las obligaciones y derechos del titular del Documento Nacional de Identidad y al 16.1, en el que se

concretan los supuestos en que las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas ("Cuando existan indicios de que han podido participar en la comisión de una infracción, cuando resulte necesario para prevenir un delito…"), y se hace alusión al estricto respeto a los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social, que necesariamente ha de regir la práctica de la diligencia de identificación.

En relación con lo preceptuado Ley Orgánica 4/2015 de 30 de marzo, la Dirección General de la Policía considera que la actuación policial se desarrolló con absoluto respeto a los principios contenidos en el artículo 16.1 LOPSC (proporcionalidad, igualdad de trato y no discriminación), siendo de reseñar que no consta que estos extremos hayan sido cuestionados por el reclamante, centrándose la reclamación únicamente en el medio usado para la práctica de la identificación. El artículo 16.2 LOPSC, contempla el uso de cualquier medio al alcance de los agentes que favorezca el acto de la identificación.

En este sentido, la funcionaria que practicó la diligencia de identificación utilizó los medios disponibles a su alcance, atendiendo a las circunstancias excepcionales del contexto de pandemia internacional motivado por el coronavirus SARS-CoV-2, al objeto de practicar la identificación con un medio que facilitó la intervención reduciendo al máximo el contacto interpersonal, ello como se ha dicho anteriormente, siguiendo las indicaciones de las autoridades sanitarias al respecto.

Una vez hechas las comprobaciones necesarias, las imágenes fueron borradas sin que de las mismas quedara rastro alguno en ningún fichero policial.

Asimismo, se considera que la actuación policial en el marco de la prevención delictual y mantenimiento del orden público se acomodó específicamente a los principios básicos de actuación establecidos en el artículo 5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, así como a las previsiones de la propia LOPSC.

SEGUNDO.- La actuación que da origen al presente procedimiento, consiste en la diligencia de identificación que tal y como se desprende de los artículos antes referenciados de la LOPSC, forma parte de la actividad que, en materia de prevención de infracciones penales y administrativas, realizan las Fuerzas y Cuerpos de Seguridad. Conviene señalar que los eventos que aglutinan grandes concentraciones de personas, como el que es objeto de análisis, suelen ser aprovechados por individuos o grupos que, amparados en la multitud protagonizan hechos delictivos que deben ser prevenidos por las FFCC Seguridad para garantizar la seguridad ciudadana y el libre desarrollo de los derechos fundamentales y libertades públicas del resto de ciudadanos.

TERCERO.- El acto que da origen al presente procedimiento, consiste en la diligencia de identificación realizada en el transcurso de la concentración celebrada en el distrito madrileño de San Blas, el día 1 de junio de 2.021. La

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, alegada por la AEPD para incoar el procedimiento sancionador, excluye expresamente de su ámbito de aplicación en su artículo 2.2 a los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

El artículo 2.2.d) del RGPD regula el ámbito de aplicación material de este, y excluye al tratamiento de datos personales realizado 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.

El 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, en el momento de los hechos que originan el presente procedimiento sancionador, continuaban siendo objeto de regulación por los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en virtud de lo previsto en la Disposición adicional 14 LPDGDD.

Por otro lado, en lo que al uso de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad se refiere, el marco normativo venía dado por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que, no obstante, no refería en su articulado ninguna limitación ni exigía autorización alguna respecto del uso de cámaras fotográficas.

CUARTO.- El Acuerdo de inicio de procedimiento sancionador, en su punto IV, analiza el presunto tratamiento excesivo de datos personales de los manifestantes, y alude a una supuesta vulneración de lo prescrito en el artículo 5 LPDGDD, 1.c) se especifica que "el tratamiento de los datos personales debe ser adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados", conocido como principio de minimización de datos.

QUINTO.- el Acuerdo de inicio, concluye que, los hechos conocidos podrían ser constitutivos de una infracción al artículo 32.1 RGPD: "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: (…) b).- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento", y en este caso, donde el agente realizó una fotografía del DNI del reclamante con su teléfono móvil de uso personal, no garantiza en absoluto lo estipulado en este artículo".

El mencionado criterio no es compartido por la Dirección Adjunta de la Dirección General de la Policía, dadas las circunstancias en las que se realizó la identificación, dado que la exposición del documento por parte de su titular al agente y la consiguiente copia de los datos por este último, requería necesariamente un espacio temporal de contacto estrecho más amplio que el tiempo que precisa la realización de la fotografía al documento, siendo esta última opción, la elegida por la funcionaria actuante dadas las circunstancias sanitarias existentes en el momento de la actuación, y por otro lado, el borrado instantáneo de los datos del terminal por el que fueron capturados, garantiza la minimización de los riesgos en el tratamiento.

Sí bien, si era posible una recogida de los datos menos invasiva, pero esta posibilidad redundaría en perjuicio de la seguridad de los agentes y particulares, al ampliar el tiempo de contacto interpersonal, y en el caso de los agentes, este incremento del riesgo se eleva exponencialmente en actos multitudinarios como el que ocasionó la identificación que ahora se evalúa, sin perjuicio de que en contra de su voluntad y en cumplimiento de sus obligaciones, puedan asimismo actuar como vectores de contagio.

Por ello, se considera acreditada la necesidad e idoneidad del medio empleado en esta específica actuación a los efectos de reducir los tiempos de contacto interpersonales, y mantener la distancia social que las autoridades sanitarias venían exigiendo, y que la identificación policial, no vulneraría el principio de minimización de datos.

SEXTO.- Finalmente, y en lo referente a la calificación de los hechos, los mismos se incardinan en la falta grave, tipificada en el artículo 73.f) de la LOPDGDD, que recoge la infracción consistente en: "f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del RGPD".

Esta conducta no coincidiría con los hechos enjuiciados, en tanto en cuanto la diligencia de identificación desarrollada por los agentes estaba únicamente orientada a la prevención de hechos tipificados como delito a la vista de hechos con antecedentes y causas similares, siendo por el contrario actuaciones policiales amparadas en la LOPSC y ejecutadas en base al principio de proporcionalidad, idoneidad y mínima intervención, dado que únicamente pretendían garantizar la seguridad ciudadana y evitar la consumación de hechos delictivos mediante la prevención, garantizando con el borrado instantáneo de las imágenes el nivel de seguridad adecuado al tratamiento de los datos llevado a cabo en la situación de pandemia".

SÉPTIMO: Con fecha 22/02/22, se inició el período de práctica de pruebas, acordándose en el mismo: a).- dar por reproducidos a efectos probatorios la denuncia interpuesta por la denunciante y su documentación, los documentos obtenidos y generados que forman parte del expediente E/07313/2020 y b).- dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del PS/00509/2021, presentadas.

OCTAVO: Con fecha 10/03/22, se da traslado a la DGP la propuesta de resolución, en la cual, se proponía que, por parte de la Directora de la Agencia Española de Protección de Datos se dirigiera un apercibimiento a dicho Organismo, por la infracción del artículo 32.1 del RGPD, al realizar un tratamiento de los datos personales del reclamante, mediante la toma de una fotografía de su DNI con un teléfono móvil personal del agente de policía, sin las garantías de seguridad exigibles para este tipo de actos.

NOVENO: Notificada la propuesta de resolución a la DGP, ésta, con fecha 17/03/22, presenta escrito de alegaciones, indicado, entre otras, lo siguiente:

I.- Respecto de la diligencia de identificación.

La Ley Orgánica 4/2015 de 30 de marzo, de protección de la seguridad ciudadana (en adelante, LOPSC), haciendo alusión, en primer lugar al preámbulo donde se indica que "…se habilita a las autoridades competentes para acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación…".

En los artículos 9 de la misma norma, sobre las obligaciones y derechos del titular del Documento Nacional de Identidad y artículo 16.1, se concretan los 3 supuestos en que las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas ("Cuando existan indicios de que han podido participar en la comisión de una infracción, cuando resulte necesario para prevenir un delito…"), y se hace alusión al estricto respeto a los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social, que necesariamente ha de regir la práctica de la diligencia de identificación.

Sobra decir que la actuación policial se desarrolló con absoluto respeto a los principios contenidos en el artículo 16.1 LOPSC (proporcionalidad, igualdad de trato y no discriminación), extremos que no ha cuestionado el reclamante, centrándose la queja de este únicamente en el medio usado para la práctica de la identificación.

El uso de dispositivos electrónicos es cada vez más usual en los diferentes servicios policiales y su finalidad es la de agilizar las actuaciones policiales, optimizando los recursos disponibles sin menoscabo de las garantías ciudadanas y reduciendo los tiempos de intervención, lo cual redunda en los estándares de calidad del servicio policial y en la seguridad de los propios actuantes.

El artículo 16.2 LOPSC, sí que contempla el uso de cualquier medio al alcance de los agentes que favorezca el acto de la identificación. Artículo 16.2 LOPSC.- Cuando no fuera posible la identificación por cualquier medio, incluida la vía

telemática o telefónica, o si la persona se negase a identificarse, los agentes, para impedir la comisión de un delito o al objeto de sancionar una infracción, podrán requerir a quienes no pudieran ser identificados a que los acompañen a las dependencias policiales más próximas (…).

En base a esta habilitación, que refiere el uso de cualquier medio, sin ceñirse estrictamente a medios oficiales o de dotación, la funcionaria que practicó esta diligencia, utilizó los medios disponibles a su alcance, en este caso un dispositivo móvil particular, por no disponer en ese momento de otro dispositivo oficial a su disposición, y atendiendo a las circunstancias excepcionales del contexto de pandemia internacional motivado por el coronavirus SARS-CoV-2, al objeto de practicar la identificación con un medio que facilitó la intervención reduciendo al máximo el contacto interpersonal, ello como se ha dicho anteriormente, siguiendo las indicaciones de las autoridades sanitarias al respecto y con un escrupuloso respeto a la normativa de protección de datos en lo que se refiere al tratamiento de estos datos personales pues, como ya se indicó, una vez hechas las comprobaciones necesarias, las imágenes fueron borradas sin que de las mismas quedara rastro alguno en ningún fichero policial o privado.

4 Puede afirmarse, por tanto, que la actuación policial de prevención delictual y mantenimiento del orden público se acomodó específicamente a los principios básicos de actuación establecidos en el artículo 5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, así como a las previsiones de la propia LOPSC.

II.- Normativa de aplicación en materia de protección de datos personales.

El acto que da origen al presente procedimiento consiste en la diligencia de identificación que se realizó en el transcurso de una concentración en Madrid, el día 01/06/21.

La diligencia de identificación, tal y como se extrae de los artículos antes referidos de la LOPSC, forma parte de la actividad que, en materia de prevención de infracciones penales y administrativas, realizan las Fuerzas y Cuerpos de Seguridad. Conviene señalar nuevamente que muchas concentraciones o manifestaciones, suelen ser aprovechadas por individuos o grupos que amparados en la multitud protagonizan hechos delictivos que deben ser prevenidos por las Fuerzas y Cuerpos de Seguridad para garantizar la seguridad ciudadana y el libre desarrollo de los derechos fundamentales y libertades públicas del resto de ciudadanos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, alegada por la AEPD para incoar el procedimiento sancionador, excluye expresamente de su ámbito de aplicación a esta materia, determinando en el artículo 2.2 de la misma:

Artículo 2 LPDGDD.- 2. Esta ley orgánica no será de aplicación: a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de

protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

En este sentido, el artículo 2.2.d) del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2.016, 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, regula el ámbito de aplicación material del mismo, y excluye al tratamiento de datos personales realizado 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.

Por todo lo anterior, las referencias que en la Propuesta de Resolución de Procedimiento Sancionador se realizan a esta Ley Orgánica 3/2018, de 5 de diciembre, son incorrectas, en la medida en que la materia sobre la que versa se encuentra excluida expresamente de su ámbito de aplicación.

De este modo no cabe duda de que, en la fecha en que suceden los hechos objeto del presente procedimiento, el 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, en el momento de los hechos que originan el presente procedimiento sancionador, ya eran objeto de regulación por 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, dictada en trasposición de 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.

III.- Respecto al fondo del asunto:

Sin perjuicio de lo anterior, y de la clara exclusión de la LPDGDD por exceder del ámbito de aplicación de la materia tratada, la Propuesta de Resolución realiza en el Fundamento de Derecho III, un análisis sobre el presunto tratamiento excesivo de datos personales de los manifestantes: alcanzando la siguiente conclusión:

(…) Que dado el contexto social-sanitario a causa de la pandemia que estábamos padeciendo, se valoró el alto riesgo de contagio por el virus Covid-19, el cual se ha constatado que se multiplica en estos actos multitudinarios, por lo que procedió a realizar una fotografía del DNI del reclamante el único objetivo de evitar la manipulación de este y mantener la distancia de seguridad y que, una vez hechas las comprobaciones necesarias, lo borró inmediatamente del dispositivo. Para matizar a continuación que, "el hecho de que se aconsejara extremar precauciones y agilizar en todo lo posible las

intervenciones con los manifestantes, utilizando un medio excepcional de identificación como es hacer fotografías con un teléfono móvil posibilitó que, en la labor de identificación de los manifestantes se redujera el contacto interpersonal entre ellos y los agentes. Todo ello unido a que, una vez hechas las comprobaciones necesarias en la identificación, las imágenes tomadas con el móvil fueran borradas.

Finalmente considera la citada resolución que "la realización de la fotografía del DNI del reclamante, en las circunstancias tan excepcionales de pandemia vividas, cumple con el principio de minimización del dato, recogido en el artículo 5.1.c) del RGPD, esto es: "adecuados, pertinentes y limitados a la necesidad", para la que fueron recabados."

En el siguiente Fundamento Jurídico, se analiza la toma de fotografía del DNI del reclamante con el teléfono móvil particular de la agente de Policía Nacional: en este sentido, considera acreditado el hecho de que la fotografía del DNI del particular fue realizada con el teléfono móvil particular de la funcionaria de policía.

Respecto de esta circunstancia, desde la Dirección Adjunta Operativa de la DGP, ya se han impartido instrucciones al objeto de asegurar la conformidad de las actuaciones policiales con la normativa en materia de Protección de Datos, instrucciones que fueron difundidas a todas las unidades policiales para su conocimiento.

Se hace referencia en este Fundamento de Derecho, al artículo 32 del RGPD, que exige a los responsables del tratamiento la adopción de las correspondientes medidas de seguridad de índole técnica y organizativa necesarias que garanticen que el tratamiento es conforme a la normativa vigente, así como garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo los pueda tratar siguiendo instrucciones del responsable.

A continuación hace referencia al apartado 1.b) del citado artículo 32, que refiere lo siguiente: "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: (…) b).- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas de tratamiento".

Concluyendo finalmente que: "en este caso, donde la agente de policía realizó una fotografía del DNI del reclamante con su teléfono móvil de uso personal, no garantiza un nivel de seguridad adecuado a las exigencias requeridas, circunstancia que no ocurriría si dicha fotografía hubiera sido realizada con un dispositivo oficial.

”PRIMERO.- La Ley Orgánica 7/2021, a la que anteriormente se ha hecho referencia respecto a su aplicación preferente por ser ley especial respecto a la normativa general de protección de datos personales tratados por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, así como la Directiva del Parlamento Europeo y del Consejo, 680/2.016, también contienen regulación propia respecto a la seguridad del tratamiento, así el 7 artículo 37 de la LO 7/2021 se determina que: 1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13.

Este artículo no hace mención, a la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas de tratamiento, que se menciona en la resolución de la Agencia y que sí contiene el RGPD.

Sin embargo, sí hace mención expresa a que han de tenerse en cuenta diferentes circunstancias como: el contexto del tratamiento, al que tantas veces se ha aludido en el desarrollo del presente procedimiento, el contexto en el que desenvuelve la identificación en cuestión fue un contexto completamente anómalo, en el que la situación de pandemia mundial provocada por el COVID, exigía que las medidas de protección de la salud tanto de los agentes de policía como de los particulares, se interpusieran a otras circunstancias en otros contextos prioritarias, haciendo que hubieran de relajarse ciertos protocolos y modos de actuación a fin de dar prioridad a la seguridad sanitaria.

Este contexto, hay que matizar que apareció de forma tan inopinada y sobrevenida, que no posibilitó la adopción por parte de las Administraciones Públicas, de medios técnicos suficientes para garantizar que todos los funcionarios dispusieran de las herramientas oficiales aptas para garantizar que estas funciones de protección y prevención de la seguridad ciudadana en entornos multitudinarios se desarrollaran con los medios que en materia de tratamiento de datos serían deseables. De este modo, quedó a criterio de los funcionarios la adopción de las medidas que en su caso consideraron oportunas para proteger su seguridad y la de los particulares, siempre actuando bajo los principios de legalidad y responsabilidad exigidos por el art. 6 de la L.O. 2/1986, de 13 de mayo, de Fuerzas y Cuerpos de Seguridad, y con respeto a los derechos de los particulares relativos al tratamiento de sus datos personales.

También hace alusión este artículo a los niveles de riesgo para los derechos y libertades de las personas físicas. En este sentido, hay que pararse a analizar las circunstancias concretas que rodearon la actuación policial. Por un lado, las medidas técnicas de seguridad del dispositivo utilizado (el teléfono particular de la funcionaria), una vez consultada la Jefatura Superior de Policía sobre este

extremo, informa que el terminal utilizado disponía de las siguientes medidas de seguridad:

1.- Cifrado de todos los datos personales, protegido por tecnología "protección de datos" mecanismo por el que se protegen los archivos y el llavero de este, contraseña con clave, así como por FACEID, no pudiendo acceder al terminal móvil sin ellos.

2.- El terminal móvil durante toda la captación, así como traslado de los datos a otro soporte se encontraba sin conexión a internet.

3.- Que así mismo no se tiene activada conectividad alguna entre la galería de fotos y las aplicaciones de almacenamiento en la nube ni ninguna otra aplicación de terceros.

4.- Reiterar que, la captación de estos datos personales, se hicieron sin la imagen fotográfica del titular del documento, siendo por tanto datos idénticos a los que se hubieran hecho en formato escrito.

5.- Se quiere reseñar, además, que la toma de datos en formato papel muestra más carencias de seguridad que la toma con medios tecnológicos, como puede ser la imposibilidad de su eliminación inmediata al tener que contar con contenedores especiales para su destrucción, así como seguridad en caso de extravío.

Además de lo anterior, hay que tener en cuenta los siguientes factores:

a) El plazo de conservación de los datos personales del particular: a la vista del informe remitido por la agente procedió a borrar la imagen del documento una vez cumplida la finalidad para la cual se tomó, es decir, que los datos fueron obtenidos y conservados durante escasos minutos, tiempo que tardó en llevarse a cabo la efectiva identificación del particular, transcurrida la cual, fueron suprimidos del dispositivo sin que quedara ningún rastro de almacenamiento del mismo o en ningún otro fichero.

b) La constante custodia de los datos por parte de una agente de Policía Nacional. Toda vez que la fotografía no fue remitida a ningún otro dispositivo, no saliendo en ningún momento del dispositivo particular de la funcionaria y por ende de su ámbito de control, hecho que, unido al resto de medidas de seguridad de que contaba el dispositivo utilizado asegura notablemente la seguridad del tratamiento.

c) Hay que considerar también, que la alternativa a este proceder de la funcionaria hubiera sido la copia manuscrita de los datos del particular para a continuación comunicarlos a través de la emisora y realizar las comprobaciones oportunas. En primer lugar, significar que esta opción requiere un tiempo de contacto interpersonal superior al de la realización de la fotografía (dado que se pretendía evitar en la medida de lo posible la manipulación por los funcionarios de cientos de documentos de identidad), y por tanto mayor riesgo de contagio.

Por otro lado estos datos manuscritos, también quedan bajo la custodia particular de la funcionaria, responsable en su caso de su pérdida o extravío, si bien, respecto a estas 9 actuaciones, se atiende a la responsabilidad de los funcionarios policiales, quienes se encuentran sometidos a un estatuto profesional, régimen disciplinario y códigos éticos, conteniendo unos estrictos principios básicos de actuación; estamos hablando (entre otros) de los principios contenidos en la L.O. 2/1.986, de 13 de mayo, de Fuerzas y Cuerpos de Seguridad, en concreto, el principio de responsabilidad (art. 5.6) según el cual los funcionarios policiales "son responsables personal y directamente por los actos que en su actuación profesional llevaren a cabo, infringiendo o vulnerando las normas legales, así como las reglamentarias que rijan su profesión y los principios enunciados anteriormente, sin perjuicio de la responsabilidad patrimonial que pueda corresponder a las Administraciones Públicas por las mismas.".

En el presente caso, se puede afirmar a la vista del resultado de los hechos que la funcionaria actuó en todo momento bajo el citado principio de responsabilidad, y prueba de ello, es que los datos personales del particular fueron tratados con el único objeto de la prevención de la seguridad ciudadana (art. 1 de la LO 7/2021), y garantizando que el particular no sufriera ningún daño derivado del citado tratamiento.

SEGUNDO.- El artículo 83 del Reglamento General de Protección de Datos establece las condiciones generales para la imposición de multas administrativas. En el apartado segundo del mismo, se determina lo siguiente: Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido; el propósito del tratamiento viene fundado en el cumplimiento de las labores de prevención de la seguridad ciudadana para el que la Ley Orgánica 4/2015, atribuye competencias a las FFCCSS, ordenando la utilización de los medios al alcance a fin de garantizar la identificación de personas con objeto de asegurar la prevención y mantenimiento de la seguridad ciudadanas, es decir, los datos personales no fueron tratados para otros fines distintos de los establecidos en el art. 1 de la LO 7/2021, de 26 de mayo. La gravedad de la infracción ha de estimarse como nimia, a la vista de la ausencia de daños en la persona titular de los datos, lo mismo cabe decir respecto a la duración de la infracción, una vez acreditada la brevedad del tratamiento.

b) la intencionalidad o negligencia en la infracción; no se aprecia por esta parte ningún tipo de negligencia en el actuar de la funcionaria de policía, toda vez que la 1 De aplicación supletoria a la LO 7/2021, tal y como se deduce del art.2.3 LOPDGDD cuando dispone que "los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea,

se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley Orgánica". 10 actuación se realizó con todas las medidas de seguridad necesarias para garantizar el buen fin de la intervención policial, la seguridad de los datos personales, y lo que es más importante, salud de los funcionarios y particulares.

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; como ya se ha adelantado, el particular no sufrió daño alguno derivado del tratamiento de sus datos personales, pero a fortiori, la Dirección Adjunta Operativa ha adoptado medidas para evitar la utilización de dispositivos electrónicos particulares en orden a la identificación de personas, las cuales han consistido, por un lado, en la difusión a todo el ámbito de esta Dirección, de instrucciones operativas referidas a la práctica de identificaciones, y por otro lado, se encuentra en estado avanzado de elaboración, de una disposición normativa de carácter general que regulará el uso de dispositivos de grabación móviles por parte de los funcionarios policiales, a fin de adaptar los nuevos protocolos, a los postulados de la L.O. 7/2021, de 26 de mayo.

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) Toda infracción anterior cometida por el responsable o el encargado del tratamiento; No se tiene constancia de la existencia de denuncias por hechos similares, siendo esta medida excepcional y derivada de la situación transitoria provocada por la situación de pandemia provocada por el virus COVID SARS 19, por lo que se puede afirmar que no ha existido reincidencia en estos hechos.

f) El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción: En este sentido hay que precisar que no ha sido necesaria ninguna actividad complementaria destinada a mitigar los efectos adversos dado que no se ha producido daño alguno. Todos los esfuerzos de la autoridad de control se han centrado en la adopción de medidas preventivas destinadas a la regulación del uso de dispositivos electrónicos y su adaptación a la reciente normativa de protección de datos. g) las categorías de los datos de carácter personal afectados por la infracción. Tal y como informa la funcionaria de Policía, la fotografía del documento se limitó a los datos personales relativos a: Nombre, apellidos, sexo, nacionalidad, fecha de nacimiento, emisión del documento y validez, así como número de soporte y número de documento, sin que fuera fotografiada la imagen del mismo, por ende, no se han tratado categorías especiales de datos, cuya protección se encuentra reforzada por la ley, a pesar de la habilitación expresa para su tratamiento por parte de las Fuerzas y Cuerpos de Seguridad, prevista en el art. 13 de la LO 7/2.021.

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso,

en qué 11 medida; Si bien es cierto que, la autoridad de control tuvo conocimiento de los hechos que conforman la presunta infracción por denuncia del particular, y no por esta Dirección, ello se debe principalmente a que atendiendo a los fundamentos jurídicos que se exponen en el presente escrito, no se aprecia falta administrativa alguna en la práctica de la identificación del particular, dado el excepcional contexto en el que fue desarrollada la misma. Destacar por otro lado, que además de admitirse la realidad de los hechos, todas las actuaciones han ido encaminadas desde su conocimiento a reforzar la prevención de conductas que pudieran ser contrarias a la normativa reguladora de protección de datos personales.

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción. En este sentido alegar que la única ventaja resultante del modo de actuar de la funcionaria de policía, puede derivarse para la seguridad ciudadana, así como para la seguridad y salud de los implicados en la intervención policial (funcionarios y particulares), pues la finalidad de esta decisión no fue otra que la de facilitar la identificación de esta persona, en un contexto multitudinario, evitando en lo posible el contacto, y agilizando la intervención en aras a la seguridad, sin olvidar en ningún momento la seguridad del tratamiento de los datos personales.

TERCERO.- Este artículo fue debidamente traspuesto a la normativa española, teniendo reflejo en el artículo 76 de la L.O. 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el cual establece que: 2. De acuerdo con lo previsto en el artículo 83.2.k) del RGPD para tener en cuenta: a) El carácter continuado de la infracción. No se aprecia tal carácter en la intervención objeto del presente procedimiento. b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales. El tratamiento de datos personales viene a ser competencia directa de la Dirección General de la Policía, en virtud de las competencias asignadas a este cuerpo policial por la L.O. 2/1986, de 13 de mayo de Fuerzas y Cuerpos de Seguridad, así como por la L.O. 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. c) Los beneficios obtenidos como consecuencia de la comisión de la infracción. Sobra decir que no se ha obtenido mayor beneficio con la intervención realizada más allá del derivado para la seguridad ciudadana y la salud de los implicados. d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción. e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente. f) No se han visto afectados derechos de menores. g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos. h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de

resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

En base a todo lo expuesto, y atendiendo a todas estas circunstancias analizadas, que el artículo 83 insta a considerar a la hora de decidir acerca de la imposición de una sanción administrativa, se puede concluir que la actuación de la policía se ajustó a las necesidades contextuales.

Por tanto, acreditada la necesidad e idoneidad del medio empleado a los efectos de reducir los tiempos de contacto interpersonales, y mantener la distancia social que las autoridades sanitarias impusieron a fin de prevenir sucesivos contagios, y a la vista de las medidas de seguridad adoptadas en el desarrollo de la intervención analizada, esta Dirección General entiende que la identificación del particular, estuvo revestida de las garantías de seguridad exigibles, no procediendo por tanto, la imposición de la sanción de apercibimiento propuesta por el órgano instructor, por lo que se insta al archivo del presente procedimiento sin imposición de sanción alguna".

De las actuaciones practicadas en el presente procedimiento, de la información y documentación presentada por las partes, han quedado acreditados lo siguiente:

HECHOS PROBADOS

Primero: El reclamante, cuando intentó abandonar la manifestación en la que estaba participando, un control policial que se encontraba en una de las calles adyacentes a la manifestación les requirió que se identificara. Cuando les mostró el DNI, uno de los agentes realizó una fotografía del documento y se lo devolvió.

Segundo: La DGP, ante estos hechos manifestó a esta Agencia, entre otras que, el tratamiento de datos realizado por la agente de policía al realizar la fotografía del DNI del reclamante con la cámara de su teléfono móvil particular fue un modo de proceder excepcional en las circunstancias de pandemia vividas, a fin de evitar un riesgo para su salud.

Tercero: La DGP afirma ante esta Agencia que, desde la Dirección Adjunta Operativa, se procederá a impartir instrucciones sobre el uso de dispositivos electrónicos por parte de funcionarios policiales en actuaciones operativas, de manera que se asegure la conformidad de dichas actuaciones a la normativa en materia de Protección de Datos.

FUNDAMENTOS DE DERECHO

I.- Competencia:

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD en el art. 47 de LOPDGDD.

II.- Síntesis de los hechos:

Según el reclamante, cuando intentó abandonar la concentración en la que estaban participando, un control policial que se encontraba en una de las calles adyacentes a la concentración le requirió que se identificara. Cuando les mostró su DNI, uno de ellos realizó una fotografía del documento con su teléfono móvil personal y se lo devolvió. El reclamante asegura que la propia agente le manifestó que las fotografía se estaba tomando con su teléfono móvil personal, ya que, no tenían teléfono de dotación oficial.

Por parte de la DGP se manifestó que, en el contexto social y sanitario como el que se estaba viviendo, marcado por el coronavirus COVID-19, la práctica de identificación de personas llevaba implícito un incremento de riesgo personal para la salud de los agentes por lo que en casos como éste, se extremaron las medidas de autoprotección evitando el todo contacto directo con las personas que se identificaban y con sus pertenencias, buscando condiciones ambientales de asepsia y manteniendo distancias de seguridad, por lo que se decidió que la mejor solución para ello, era la toma de fotografías del DNI, asegurando que, una vez hechas las comprobaciones oportunas para la correcta identificación, la fotografía era borrada inmediatamente del dispositivo.

III.- Sobre las alegaciones manifestadas por la DGP a la propuesta de resolución.

PRIMERO: La DGP alega en su escrito de fecha 17/03/22 que, el artículo 2.2.d) del RGPD, excluye de su aplicación al tratamiento de datos personales realizado 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, y que, por tanto, el tratamiento de datos realizado por la agente de policía al realizar la fotografía del DNI del reclamante con la cámara del teléfono móvil particular se encuentra excluida expresamente del ámbito de aplicación del RGPD y de la LOPDGDD.

Respecto a esto se debe indicar lo siguiente:

la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (LOPSC), habilita a las autoridades competentes para:

> *"(…) acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación (…)".*

En aplicación de lo anterior, el artículo 9.2 de la LOPSC, establecen, respecto de la obligación de exhibir el DNI a los agentes de las Fuerzas y Cuerpos de Seguridad del Estado, lo siguiente:

> *"2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo y permitir la comprobación de las medidas de seguridad a las que se refiere el apartado 2 del artículo 8 cuando fueren requeridas para ello por la autoridad o sus agentes, para el cumplimiento de los fines previstos en el apartado 1 del artículo 16. De su sustracción o extravío deberá darse cuenta tan pronto como sea posible a la*

comisaría de Policía o puesto de las Fuerzas y Cuerpos de Seguridad más próximo".

Por su parte, el artículo 16 de la propia LOPSC, sobre la posibilidad de comprobación del DNI por parte de las Fuerzas y Cuerpos de Seguridad del Estado, establece que:

1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:

a) Cuando existan indicios de que han podido participar en la comisión de una infracción.

b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito. En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados (…)".

No obstante, en la propia Ley LOPSC, se establecen ciertos límites a esta práctica de comprobación de los DNI, indicando que:

"(…) En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social (…)".

El Esquema Nacional de Seguridad, regulado en el Real Decreto 3/2010, de 8 de enero, modificado por Real Decreto 951/2015, de 23 de octubre, establece, en su artículo 21, lo siguiente:

"En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros.

Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

2.- Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

Y por su parte, el artículo 22 del RD 3/2010, sobre la prevención ante otros sistemas de información interconectados, establece lo siguiente:

"El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Sobre el Registro de Actividad, el artículo 23 del RD 3/2010, establece que:

"Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa".

Y sobre los requisitos mínimos exigidos, el artículo 27 del RG 3/2010, establece:

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta: a) Los activos que constituyen el sistema. b) La categoría del sistema, según lo previsto en el artículo 43. c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

Nota: Norma derogada, con efectos de 07/12/18, sin perjuicio de lo previsto en la disposición adicional 14 de la Ley Orgánica 3/2018, de 5 de diciembre, según establece su disposición derogatoria única) por lo que este apartado se entiende referenciado al RGPD y a la LOPDGDD, actualmente, en vigor)

3. Las medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la información, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Por último, sobre las auditorias de seguridad de los sistemas de información utilizados, el artículo 34 del RD 3/2010, establece lo siguiente:

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad. Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

2. Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.

3. En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.

4. En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

6. Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

Por tanto, teniendo en cuenta los riesgos señalados debe considerarse que el uso de cámaras o móviles personales, no oficiales o de dotación, de los agentes no garantiza la seguridad de los datos, en tanto que los usos privados que cada persona pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de

seguridad que para el ejercicio de las funciones de policía deben adoptarse por los responsables del fichero policial del que formarán parte tales grabaciones.

SEGUNDO: Sobre la afirmación que hace la DGP cuando indica que: *"(…)De este modo, quedó a criterio de los funcionarios la adopción de las medidas que en su caso consideraron oportunas para proteger su seguridad y la de los particulares, siempre actuando bajo los principios de legalidad y responsabilidad exigidos por el art. 6 de la L.O. 2/1986, de 13 de mayo, de Fuerzas y Cuerpos de Seguridad, y con respeto a los derechos de los particulares relativos al tratamiento de sus datos personales (…)".*

Se debe indicar a este respecto que, la Disposición adicional primera de la LOPDGDD, sobre la "Medidas de seguridad en el ámbito del sector público" establece que:

> *1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.*
>
> *2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.*
>
> *En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.*

La DGP, como Órgano del Ministerio del Interior le es de aplicación lo establecido en el apartado 2 de la citada disposición adicional y al ser ella, la DGP la que actúa como responsable del tratamiento de los datos personales, es su obligación aplicar a los tratamientos de datos personales realizado por sus funcionarios, las medidas de seguridad que correspondan, de las previstas en el Esquema Nacional de Seguridad, no estando aparado por la normativa, dejar *"(…) a criterio de los funcionarios la adopción de las medidas que en su caso consideraron oportunas para proteger su seguridad y la de los particulares (…)",*

TERCERO: Sobre la afirmación que hace la DGP cuando indica que. *"(…) se puede afirmar a la vista del resultado de los hechos que la funcionaria actuó en todo momento bajo el citado principio de responsabilidad, y prueba de ello, es que los datos personales del particular fueron tratados con el único objeto de la prevención de la seguridad ciudadana (art. 1 de la LO 7/2021), y garantizando que el particular no sufriera ningún daño derivado del citado tratamiento (…)".*

Indicar a este respecto que, según establece su Disposición final duodécima, esta Ley Orgánica *"entrará en vigor a los veinte días de su publicación en el Boletín Oficial del*

Estado. Su publicación se produjo el 27/05/21, por lo que la entrada en vigor de la norma se produjo el 16/06/21.

Pues bien, como los hechos objeto del presente procedimiento se produjeron el 01/06/21, fecha en la que aún no estaba en vigor la Ley Orgánica 07/2021, no es posible tenerla en consideración en este caso.

CUARTO: Sobre la consideración que solicita la DGP, en el sentido de aplicar los atenuantes indicados en el artículo 83 del RGPD y en el artículo 76 de la LOPDGDD.

Sobre este aspecto, hay que indicar que el artículo 77.2 de la LOPDGDD, establece lo siguiente:

> "*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 sancionando a las mismas con apercibimiento (…)"*,

Por lo que no es posible, en este caso, tener en consideración lo estipulado en el artículo 83 del RGPD y en el artículo 76 de la LOPDGDD, a efectos de graduar la sanción a imponer, pues en este caso, solo cabe sancionar con apercibimiento.

IV.- Sobre la infracción del artículo 32 del RGPD cometida por la DGP.

El RGPD, en su artículo 32, exige a los responsables del tratamiento la adopción, de medidas de seguridad de índole técnica y organizativa que garanticen que el tratamiento de los datos personales se realice conforme a la normativa vigente, así como que, cualquier persona que actúen bajo la autoridad del responsable o del encargado lo realice siguiendo las instrucciones del responsable y así se establece en dicho artículo:

> *1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

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

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

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

V.- Tipificación y Sanción por la infracción del artículo 32.1 del RGPD

En el presente caso, el hecho de realizar una fotografía del DNI con un teléfono móvil de uso personal de un agente de policía supone la comisión de la infracción del artículo 32.1 del RGPD, al realizar un tratamiento de datos personales sin tener las garantías necesaria de tener implementadas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

En este sentido, el artículo 73.f) de la LOPDGDD, considera “grave”, a efectos de prescripción, *“f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del RGPD”.*

Esta infracción puede ser sancionada con multa de 10.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.4.a) del RGPD.

En el presente caso, al ser la parte reclamada la Dirección General de la Policía, Órgano Directivo perteneciente a la Administración General del Estado, se debe tener presente lo establecido en el art. 83.7 del citado RGPD, donde se indica que:

"*Sin perjuicio de los poderes correctivos de las autoridades de control (…) cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".*

Pues bien, el artículo 77.2 de la LOPDGDD establece, sobre el régimen aplicable a las Entidades que forman parte de la Administración Pública, lo siguiente*:*

“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, las autoridades de protección de datos que resulte competente dictarán resolución sancionando a las mismas con apercibimiento. La resolución establecerá así mismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiere cometido".

Con arreglo a dichos criterios, se estima adecuado sancionar con apercibimiento a la Dirección General de la Policía, por la infracción del artículo 32.1 del RGPD, al considera que, la realización de la fotografía de del DNI del reclamante con un teléfono móvil personal de uno de los agentes de policía, es un acto que no garantiza un nivel de seguridad adecuado al riesgo.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

RESUELVE:

PRIMERO: SANCIONAR con APERCIBIMIENTO, a la DIRECCIÓN GENERAL DE LA POLICÍA por la infracción del artículo 32.1) del RGPD, sancionable conforme a lo dispuesto en el art. 83 de la citada norma, respecto de la falta de seguridad en el tratamiento de los datos personales puesta de manifiesto a la hora de tomar una fotografía del DNI del reclamante con un teléfono móvil personal del agente de policía que realizó la identificación.

SEGUNDO: NOTIFICAR la presente resolución a la DIRECCIÓN GENERAL DE LA POLICÍA y al reclamante sobre el resultado de la reclamación.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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