- **Expediente nº.: RR/00162/2023**

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por ***ILUNION SEGURIDAD, S.A.*** (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 14 de febrero de 2023, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 14 de febrero de 2023, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente PS/00452/2022, en virtud de la cual se imponía a ***ILUNION SEGURIDAD, S.A.*** las sanciones siguientes:

- por una infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de 10.000 € (diez mil euros).

- por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD una sanción de 5.000 € (cinco mil euros).

Dicha resolución, que fue notificada a la parte recurrente en fecha 15 de febrero de 2023 fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00452/2022, quedó constancia de que se han enviado comunicaciones laborales por correo electrónico sin utilizar la opción de envío con copia oculta revelándose las direcciones de correo electrónico personales de los trabajadores a todos los destinatarios de los correos.

TERCERO: La parte recurrente ha presentado en fecha 15 de marzo de 2023, en esta Agencia Española de Protección de Datos, recurso de reposición, fundamentándolo, básicamente en los aspectos ya indicados a lo largo del procedimiento sancionador objeto de recurso, argumentando que los servicios de seguridad privada que presta ILUNION SEGURIDAD, S.A., se hallan generalmente deslocalizados y a fin de mantener informados a los trabajadores acerca de circunstancias esenciales de su relación laboral, como sus turnos, suplencias, vacaciones, prevención de riesgos laborales, formación, etc., se hace necesario mantener unos canales de comunicación ágiles y efectivos basados en el teléfono o en el correo electrónico, pues la comunicación por carta postal resulta imposible dados los tiempos que requiere. Por otro lado, afirma, que a veces puede resultar necesario que la información sea compartida entre varios trabajadores, a fin de que todos ellos conozcan que los demás

están asimismo informados de lo mismo, y resolver dudas generales. A tal efecto, en fecha 22/11/2019, se crea el grupo de WhatsApp “REFRESCO”, con los números de teléfono de un pequeño conjunto de trabajadores, que estos ya habían dado a la empresa como datos de contacto, al igual que el correo electrónico, en el marco de su relación laboral. dicho grupo sólo es utilizado para cuestiones relativas a la relación laboral, esto es, para la formación de dicho grupo de trabajadores. En ningún momento es utilizado para dar instrucciones diarias de trabajo, encargar tareas, etc.

Expresa que los trabajadores se muestran conformes con el canal de comunicación así establecido, participando en él, lo que es prueba de un comportamiento activo en aceptar que se utilice su número de teléfono en el grupo de WhatsApp. Añade que salvo por la creación de este grupo, el resto de las comunicaciones se producen por WhatsApp de forma individual. En todas las comunicaciones individuales por WhatsApp que aporta el denunciante, puede advertirse que el trabajador participa activamente aceptando, por consiguiente, el medio de comunicación establecido, y por consiguiente, el tratamiento del dato personal de su teléfono de esta forma.

Afirma que los mensajes de WhatsApp se hacen más frecuentes a partir de marzo 2020 fecha en la que fue declarado el confinamiento derivado de la pandemia lo que hizo que el envío de mensajes por WhatsApp fuera el más adecuado para trasladar los cambios de última hora a fin de mantener un servicio crítico en esos momentos como era el de vigilancia de los aeropuertos y derivados de la situación de ERTE existente en ese momento que hicieron necesario una continua reasignación de turnos de prestación del trabajo.

Fundamenta la base de legitimación para el uso del número de teléfono móvil en lo establecido en el artículo 6.1, apartados a), b) y f) del RGPD por la existencia de una relación contractual y un interés legítimo.

Argumenta que los trabajadores consintieron en el tratamiento de los datos, tanto la modalidad grupal en la que cada uno accedía al dato del teléfono de los demás, como en la comunicación individual; que el tratamiento queda amparado asimismo en el artículo 6.1.b) del RGPD como se desprende de la resolución de la AEPD R/00026/2021 y de la SAN 2087/2020, de 29 de julio; y que existió un interés legítimo, de acuerdo con lo previsto en el artículo 6.1.f) RGPD, en tratar dichos datos a la vista de dicha necesidad
provocada por la pandemia.

Finalmente alega la falta de culpabilidad de la entidad y explica que a fin de evitar que se produjeran incidencias similares, ILUNION SEGURIDAD, S.A., tomó la decisión de adoptar la medida consistente en remitir un comunicado a todos sus mandos intermedios a fin de recordar que en ILUNION SEGURIDAD, S.A. están prohibidas tanto la creación de grupos de WhatsApp con los números de teléfono particular de los trabajadores como la remisión de correos sin emplear la opción de copia oculta (CCO) a las direcciones de correo electrónico particular de dichos trabajadores, al que, además, se han acompañado a efectos igualmente recordatorios las directrices que rigen en ILUNION para el uso responsable de aplicaciones de mensajería instantánea como WhatsApp.

Asimismo, se indica que se está sancionando dos veces por el mismo hecho, cuando sólo existe una supuesta actuación infractora, lo que determina una manifiesta vulneración del principio non bis in ídem; sin perjuicio que, de tratarse de dos infracciones (que no es el caso) concurriría un concurso ideal medial de infracciones que exige imponer la sanción correspondiente a la infracción más grave (art. 29.5 Ley 40/2015).

Finalmente manifiesta la desproporción de las sanciones impuestas por un total de 15.000€ a la vista de la incorrecta graduación de la sanción, derivada de falta en consideración de los atenuantes concurrentes en los hechos y circunstancias del caso, y de la extemporánea y sorpresiva fundamentación de la agravación de la sanción en una pretendida negligencia de mi representada que vulnera sus derechos de defensa; y a la vista de supuestos parecidos en los que se ha sancionado hechos de mayor gravedad con sanciones mucho más atenuadas.

FUNDAMENTOS DE DERECHO

I
Competencia

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

II
Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, debe señalarse el importante esfuerzo argumental realizado por el recurrente con la finalidad de defender la legalidad de la creación de un grupo de Whatsapp y la utilización de este canal para la realización de comunicaciones corporativas. A este respecto, conviene recordar que no son esos los hechos sancionados por la resolución recurrida. Por el contrario, las infracciones comprobadas se refieren al hecho de haberse enviado un correo electrónico sin utilizarse la funcionalidad “con copia oculta”. Como se razona en la resolución, esto ha implicado tanto la vulneración del principio de confidencialidad establecido en el artículo 5.1.f) del RGPD como de la obligación de establecimiento de las necesarias medidas de seguridad prevista en el artículo 32 del mismo texto legal.

La parte reclamada reitera básicamente las alegaciones ya presentadas a lo largo del procedimiento sancionador, sobre este particular, debe señalarse que ya fueron analizadas y desestimadas en los Fundamentos de Derecho III, IV, V y VI, de la Resolución recurrida, tal como se transcribe a continuación:

<< III

Sobre la infracción del artículo 5.1 f) del RGPD

La comunicación de datos personales de un trabajador a otros trabajadores de la empresa implica un tratamiento de datos personales y requiere legitimación para que se produzca de forma lícita dicha comunicación de datos personales, por lo que será necesario analizar en cada caso si existe base jurídica para que el empleador pueda compartir información personal de los trabajadores, para lo que también habrá que tener en cuenta la finalidad pretendida y los datos tratados.

La entidad reclamada manifiesta la existencia de consentimiento de los trabajadores en el uso de tales medios de contacto, por considerar que existe una clara acción afirmativa de los trabajadores que legitimaría su uso.

Sobre este particular debe indicarse, con carácter previo, que no cabe duda de que resulta necesario para la ejecución del contrato que el empleador disponga de alguna vía de comunicación con las personas trabajadoras, entre las que podría incluirse la utilización de mensajería instantánea o del correo electrónico. El empleador puede utilizar para mantener estas comunicaciones con los trabajadores de su empresa un medio corporativo puesto por él a disposición de los trabajadores y también podría utilizar el medio de uso personal que el trabajador haya comunicado voluntariamente a la empresa, dado que no cabe duda de que las personas trabajadores pueden facilitar voluntariamente su número de teléfono o su dirección de correo electrónico como vía de comunicación con el empleador para cuestiones relativas al trabajo, siempre que no se trate de una obligación impuesta por el empleador.

Esta cuestión se aborda en la Guía de la Agencia sobre "La protección de datos en las relaciones laborales" en los siguientes términos

> *"(…) En general, parece necesario para la ejecución del contrato que el empleador disponga de alguna vía de comunicación con las personas trabajadoras, y es imprescindible que la persona trabajadora proporcione a la empresa alguna forma de contacto. Sin embargo, el contrato de trabajo no legitima a la empresa para solicitar a la persona trabajadora todos esos datos, como ha puesto de manifiesto el Tribunal Supremo en relación con la dirección de correo electrónico o el número de teléfono personal (STS 4086/2015, de 21 de septiembre, Sala de lo Social). Es decir, la necesidad del tratamiento habrá de ponderarse caso a caso.*
>
> *Para ello, será necesario analizar en cada caso la base jurídica alegada –que podría ser el contrato de trabajo, el consentimiento o el interés legítimo del empleador-, la finalidad pretendida y los datos tratados."*

Por tanto, habrá que tener en cuenta la finalidad que se persigue por el empleador y los datos tratados en cada caso para poder determinar si en un supuesto concreto el tratamiento puede basarse en alguna base de las contenidas en el art. 6 del RGPD, que en este contexto podrían ser las contempladas en las letras a), b) y f) del art. 6.1 del RGPD. Sobre la adecuación de estas bases de legitimación para legitimar el uso por el empleador de servicios de mensajería instantánea o del correo electrónico, pueden hacerse las siguientes consideraciones:

a) En cuanto al consentimiento, puede afirmarse que cuando el trabajador se comunica voluntariamente con el empleador a través de su teléfono móvil de uso personal o su dirección electrónica personal existe un "acto afirmativo claro" de su consentimiento a recibir a través de tales medios comunicaciones sobre asuntos laborales, como ha declarado el Tribunal Superior de Justicia de Asturias, Sala de lo Social, en su sentencia de doce de abril de dos mil veintidós, siempre y cuando la utilización de estos datos personales por el empresario no venga impuesta en el contrato de trabajo, como determinó el Tribunal Supremo en la citada Sentencia 4086/2015, de 21 de septiembre, Sala de lo Social, pues en tal supuesto el trabajador no presta su "voluntario" consentimiento como explica la referida sentencia: "(…) siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las circunstancias -se trata del momento de acceso a un bien escaso como es el empleo- bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario (…)".

Así las cosas, cuando el empleador utiliza los datos de contacto personales de las personas trabajadoras y los comparte con otros trabajadores, ya sea por correo electrónico o a través de la mensajería instantánea, como medio "necesario" para el desenvolvimiento de la relación contractual existente entre empleados y empresa, el tratamiento de estos datos no puede basarse en el consentimiento, por cuanto el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (considerando 42). El empleado debe poder negar o retirar el consentimiento sin sufrir perjuicio alguno, lo que impide que esta base de legitimación sea la adecuada para fundamentar estos tratamientos con tal finalidad, pues la dinámica de la relación laboral dependería de que el empleado libremente consintiera o no el tratamiento.

b) Cuando compartir información sobre asuntos del trabajo resulte "necesaria" para la ejecución del contrato de trabajo suscrito por el trabajador y el empleador utilice medios corporativos para ello, el tratamiento de la información personal puede quedar amparado en la base de legitimación contemplada en el artículo 6.1.b) del RGPD. Si bien, en estos casos, resultará indispensable que la información que se comparta sea adecuada, pertinente y limitada a lo necesario en relación con los fines que se persiguen, como exige el principio de minimización de datos, así como el establecimiento de medidas técnicas y organizativas adecuadas para evitar accesos no autorizados a la información personal que se comparte, a fin de no vulnerar el principio de integridad y confidencialidad recogido en el artículo 5.1.f) del RGPD.

En este sentido decíamos en la resolución del expediente EXP202105690, que archivó la reclamación de un trabajador referida a la creación de dos grupos de WhatsApp y su inclusión en los mismos por el empleador, donde se publican datos personales relativos a las rutas de reparto, las personas que las realizan, las horas, la ubicación de las furgonetas al terminar la jornada laboral y diversa información, que "los datos objeto de tratamiento son los mínimos necesarios para la organización del trabajo particular llevado a cabo por la parte reclamada, que ha informado a los trabajadores de la finalidad del tratamiento en los grupos de WhatsApp creados con la

finalidad de utilizar esta vía de comunicación en asuntos relacionados con el contrato de trabajo, condiciones laborales, organización y desarrollo de tareas de trabajo y reparto y manteniendo la confidencialidad sobre ellos".

Ahora bien, el trabajador tiene derecho a mantener el control sobre los datos personales que le atañen, por tanto, cuando los datos de contacto utilizados por el empleador no sean corporativos sino de uso personal de los trabajadores, el tratamiento de tales datos incluida su revelación a otros compañeros no podrá justificarse en la base de legitimación contemplada en el artículo 6.1.b) del RGPD.

La Audiencia Nacional, sala de lo social, en su sentencia de 27 de junio de 2022, resume la doctrina sentada por la propia sala de la Audiencia y por el TS del siguiente modo:

> *1.- Que es doctrina tanto de esta Sala, como de la Sala IV del TS; la ajenidad propia del contrato de trabajo (ex art. 1.1 E.T) implica, entre otras cosas, la ajenidad en los medios, lo que implica que es el empleador el que tiene que proporcionar al trabajador los medios necesarios para el desenvolvimiento de su relación laboral(STS de 8-2-2.021- rec 84/2.019- que confirma SAN de 6-2-2.019- proc.318/2018-; SAN de 10-5-2.021- autos105/2.021).*
>
> *2.- Que, por otro lado, ya la STS de 21-9-2015 - rec259/2014- que confirma la SAN de 28-1-2014- autos 428/2013-consideró contrario a la entonces vigente normativa nacional y europea en materia de protección de datos que el trabajador se viese obligado a proporcionar su correo y su número de teléfono personal a la empresa, razonando que si los mismos resultasen esenciales para el desenvolvimiento del contrato tanto uno como otro debían ser proporcionados por la empresa al trabajador.*

Criterio que es también el seguido en la FAQ de la AEPD ¿Puede solicitar el empresario el teléfono y dirección de correo electrónico particular del trabajador?

> *"El tratamiento del dato del correo electrónico y teléfono particulares del trabajador puede ser ignorado por el empresario, dado que ninguna norma exige que el trabajador, para la adecuada perfección de su relación contractual, haya de facilitar estos datos al empresario al que presta sus servicios.*
>
> *Es decir, dicho tratamiento excedería en cuanto al mismo de lo permitido inicialmente por la normativa de protección de datos, y más concretamente, de la legitimación del artículo 6 del RGPD en base a la ejecución de un contrato. No obstante, si las circunstancias de la prestación de servicios para la empresa conllevaran una disponibilidad personal del trabajador fuera de su centro u horario de trabajo, una medida más moderada e igual de eficaz para conseguir la comunicación de la empresa con el trabajador sería la puesta a disposición del mismo de un instrumento de trabajo como sería un teléfono de empresa.*
>
> *En todo caso, sería posible que los afectados facilitaran los datos referentes a su e-mail y número telefónico particulares, si bien la recogida de estos datos habría de ser de cumplimentación voluntaria, previa la obtención del consentimiento del trabajador, que podrá oponerse posteriormente a su tratamiento ejerciendo los derechos de oposición o supresión."*

En definitiva, el tratamiento del dato del número de teléfono personal del trabajador o de su dirección de correo particular con la finalidad de mantener la relación laboral no puede considerarse "necesario" para la ejecución del contrato, como requiere el artículo 6.1.b) del RGPD, en el sentido de que el objeto principal del contrato específico con el interesado no pueda alcanzarse si no se lleva a cabo el tratamiento concreto de los datos personales en cuestión (Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados), por cuanto el empresario siempre puede proporcionar estos medios necesarios a los trabajadores. Consecuentemente, con carácter general, este uso no puede justificarse en la base de legitimación contemplada en el art. 6.1.b) del RGPD.

c) Finalmente quedaría por analizar si la base de legitimación aplicable podría ser el interés legítimo.

En relación con esta base jurídica del interés legítimo, el artículo 6.1.f) del RGPD considera lícito el tratamiento cuando "es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales (...)".

El Considerando 47 del RGPD precisa el contenido y alcance de esta base legitimadora del tratamiento:

> *"(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo".*

También es importante destacar que las autoridades públicas en el ejercicio de sus funciones no pueden fundar sus tratamientos en esta base de legitimación.

El interés legítimo del empleador podría ser una base adecuada en un contexto laboral, como reconoció el GT29, en su Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, al considerar que podría ser lícita en virtud del artículo 7, letra f) de la Directiva "La creación de una base interna de datos de contacto de los empleados de una empresa que contenga el nombre, la dirección laboral, el número de teléfono y la dirección de correo electrónico de todos los empleados, para permitir que los empleados puedan ponerse en contacto con sus compañeros de trabajo (…) si se demuestra que prevalece el interés del responsable del tratamiento y se toman todas las medidas adecuadas, incluida, por ejemplo, la consulta a los representantes de los empleados".

De acuerdo con la doctrina del Tribunal de Justicia de la Unión Europea, por todas Sentencia de 29 de julio de 2019 (Asunto C-40/17, «Fashion ID»), esta base de legitimación requiere la concurrencia de tres requisitos acumulativos, a saber (I) que el responsable del tratamiento o el tercero o terceros a los que se comuniquen los datos persigan un interés legítimo; (ii) que el tratamiento de datos personales sea «necesario» para la satisfacción del interés legítimo perseguido, y (iii) que no prevalezcan los derechos y libertades fundamentales del interesado para lo que será necesario que el responsable realice una ponderación entre el interés perseguido y los intereses o los derechos y libertades de los interesados.

Así habrá que tener en cuenta, en todo caso, al analizar si esta base jurídica contemplada en el art. 6.1.f) del RGPD puede legitimar un concreto tratamiento, que ha de existir un justo equilibrio entre el derecho a la protección de los datos personales de los trabajadores y los intereses del empleador, de modo que la utilización por el empresario de los datos personales supere el test de proporcionalidad, que ha de observarse en cualquier medida restrictiva de un derecho fundamental en su triple manifestación de idoneidad, necesidad y proporcionalidad en sentido estricto. En particular para que el tratamiento pueda superar el test de necesidad será indispensable que no hubiera sido posible utilizar un sistema de comunicación menos invasivo que el utilizado.

No cabe duda de que existe un conflicto entre el derecho del empresario y el derecho de los empleados a la protección de sus datos personales que requiere una ponderación justa entre la necesidad de proteger la privacidad del empleado y el derecho del empresario de garantizar el buen funcionamiento de la empresa

En este sentido no pueden olvidarse las especiales circunstancias que acontecieron durante la vigencia del estado de alarma declarado en nuestro país por el Real Decreto 4463/2020 de 14 de marzo de 2020.

En nuestra resolución R/00026/2021 de 14/01/2021, teniendo en cuenta tales circunstancias, decíamos lo siguiente:

> *"(…) cabe señalar que, constantemente los métodos de comunicación son cambiantes y las empresas buscan y utilizan herramientas de organización y*

planificación sencillas, fluidas, agiles, eficaces y económicas, con las ventajas que supone para establecer de comunicación con sus empleados, permitiendo un correcto y eficiente funcionamiento de la empresa

La utilización de dispositivos móviles y sus herramientas, correo electrónico u otros dispositivos o canales telemáticos, se hacen imprescindibles para aquellos empleados que llevan a cabo sus funciones fuera de la sede laboral, como en el caso que nos ocupa. Por lo tanto, las partes deben ponerse de acuerdo para buscar canales agiles de comunicación, dado que la comunicación por vía posta podrían no ser operativas en el contexto de la relación laboral con la reclamante (máxime teniendo en cuenta la emergencia sanitaria por el Covid-19), salvo la remisión de las nóminas o comunicaciones que no exijan una actuación puntual e inmediata."

En este orden de ideas cabe citar también la sentencia 2087/2020, de 29 de julio, de la Audiencia Nacional en la que se aborda, en su fundamento octavo, la licitud del mecanismo de comunicación empleado por la empresa para informar a los trabajadores, ante la imposibilidad de realizar la entrega de la comunicación de manera presencial, como consecuencia de los aislamientos impuestos por la crisis sanitaria originada por el SARS-CoV-2, con el siguiente pronunciamiento:

"OCTAVO: Como último punto de censura cuestiona el sindicato actor el mecanismo de comunicación empleado por la empresa para informar de su decisión definitiva a los trabajadores afectados por la misma, pues el uso de diferentes aplicaciones y redes permiten la libre circulación de información de manera no fehaciente.

El motivo tampoco puede tener favorable acogida por diversas razones. En primer lugar, porque no niega el sindicato actor que los trabajadores que finalmente resultaron afectados por la medida que nos ocupa no hubieran recibido de manera fehaciente la comunicación empresarial, sino que de manera genérica se afirma que "el WhatsApp, email y otras aplicaciones similares permiten la circulación de información de forma anónima". Sin embargo, esta circunstancia no se ha constatado en el caso enjuiciado, donde la empresa ha aportado diferentes correos electrónicos remitidos desde una dirección con dominio de la compañía (de cuya autenticidad no se duda, pues se reconoció por la parte actora la totalidad de documentos aportados de contrario) a trabajadores afectados por el ERTE. De hecho, se puede comprobar como en el caso de (…) (folios 8 y 9 de descriptor 134) consta hasta la firma del propio trabajador en la casilla correspondiente, lo que evidencia la efectiva recepción del documento.

Por otro lado, no hemos de olvidar las particulares circunstancias que rodearon a la tramitación del ERTE en cuestión, con un estado de alarma declarado por Real Decreto 4463/2020 de 14 de marzo de 2020, cuyo artículo 7 limitaba la libertad de deambulación de las personas pudiendo únicamente circular por las vías de uso público para la realización de las siguientes actividades: a) Adquisición de alimentos, productos farmacéuticos y de primera necesidad. b) Asistencia a centros, servicios y establecimientos sanitarios. c) Desplazamiento al lugar de trabajo para efectuar su prestación laboral, profesional o

empresarial. d) Retorno al lugar de residencia habitual. e) Asistencia y cuidado a mayores, menores, dependientes, personas con discapacidad o personas especialmente vulnerables. f) Desplazamiento a entidades financieras y de seguros. g) Por causa de fuerza mayor o situación de necesidad. h) Cualquier otra actividad de análoga naturaleza que habrá de hacerse individualmente, salvo que se acompañe a personas con discapacidad o por otra causa justificada.

En definitiva, previendo el artículo 3.1 del Código Civil que debemos de interpretar las normas conforme a la realidad social del tiempo en que han de ser aplicadas, nunca unas circunstancias fueron tan determinantes para permitir apartarse de lo que son los hábitos y usos ordinarios en las comunicaciones entre empresario y trabajador, de tal suerte que hemos de considerar que el medio empleado por la demandada para informar a los trabajadores acerca de su inclusión en el ERTE por fuerza mayor, fue un sistema adecuado atendiendo a las circunstancias concurrentes en ese momento, no constando a mayores que a través de tal canal de comunicación no quedaran salvaguardados los derechos fundamentales de intimidad de los trabajadores, ni se garantizase la autenticidad y fehaciencia de lo comunicado. La demanda, por consiguiente, ha de ser desestimada."

No obstante, las consideraciones expuestas no pueden eximir al empresario de justificar la "necesidad de la medida" y de realizar una ponderación justa entre los intereses implicados, garantizando el derecho de oposición de los interesados que deberá ser mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información, a más tardar en el momento de la primera comunicación con el interesado (art. 21.4 RGPD).

En el procedimiento PS/00078/2021 dijimos, en cuanto a la ausencia del requisito de la ponderación, lo siguiente:

Al faltar la información relativa a la prueba de ponderación, el interesado se ve privado de su derecho a conocer la base jurídica del tratamiento alegada por el responsable, y en concreto, al referirse al interés legítimo, se ve privado de su derecho a conocer cuáles son dichos intereses legítimos alegados por el responsable o de un tercero que justificarían el tratamiento sin tener en cuenta su consentimiento.

Del mismo modo, el interesado se ve privado de su derecho a alegar por qué causas dicho interés legítimo alegado por el responsable podría ser contrarrestado por los derechos o intereses del interesado. No habiéndosele dado oportunidad al interesado de alegarlos frente al responsable, cualquier sopesamiento que realice el responsable sin tener en cuenta las circunstancias que pudiera alegar el interesado a quien no se la ha permitido hacerlo estaría viciado, por ser un acto contrario a una norma imperativa.

Es difícil aceptar que un tratamiento se base en el interés legítimo del responsable cuando ese tratamiento se lleva a cabo de forma oculta.

> *No cabe, por tanto, invocar esta base jurídica del interés legítimo con ocasión de un trámite administrativo, como el de traslado de la reclamación o el de alegaciones a la apertura del procedimiento sancionador. Aceptarlo sería tanto como admitir un interés legítimo sobrevenido, o a posteriori, respecto del cual no se han respetado las exigencias previstas en la normativa de protección de datos personales y sobre el que no se informa a los interesados.*

Y en relación con el requisito de "necesidad" la resolución se refiere a él en los siguientes términos

> *En cuanto al segundo de los requisitos, sin embargo, se considera que el tratamiento de datos personales que realiza MARINS PLAYA no es necesario o estrictamente necesario para la satisfacción del interés legítimo alegado (la sentencia citada de 04/05/2017, C-13/16, Rigas Satskime, en su apartado 30, declara "Por lo que atañe al requisito de que el tratamiento de datos sea necesario, procede recordar que las excepciones y restricciones al principio de protección de los datos de carácter personal deben establecerse sin sobrepasar los límites de lo estrictamente necesario").*
>
> *Este principio, según el cual el tratamiento debe ser estrictamente necesario para la satisfacción del interés legítimo, hay que interpretarlo de conformidad con lo establecido en el artículo 5.1.c) RGPD, que hace referencia al principio de minimización de datos, señalando que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".*
>
> *De esta forma, deberán preferirse siempre medios menos invasivos para servir a un mismo fin. Necesidad supone aquí que el tratamiento resulte imprescindible para la satisfacción del referido interés, de modo que, si dicho objetivo se puede alcanzar de forma razonable de otra manera que produzca menos impacto o menos intrusiva, el interés legítimo no puede ser invocado*

Así las cosas, de acuerdo con estos criterios no cabría apreciar esta base de legitimación cuando no concurran las circunstancias expuestas, a las que habría que añadir el criterio de nuestra jurisprudencia, recogido anteriormente sobre el tratamiento del dato del número de teléfono personal del trabajador o de su dirección de correo particular con la finalidad de mantener la relación laboral, consistente en que cuando los mismos resultan esenciales para el desenvolvimiento del contrato, tanto uno como otro deben ser proporcionados por la empresa al trabajador para no quebrar con la necesaria ajenidad de los medios que caracteriza el contrato de trabajo. La exigencia de la aportación de estos medios por el trabajador podría suponer un manifiesto abuso de derecho empresarial, como se desprende de la SAN de 6 de febrero de 2019.

Sentado lo anterior y centrándonos en la infracción que se examina – quebrantamiento del deber de confidencialidad-, procede en primer lugar analizar si la creación del grupo de WhatsApp "REFRESCO" en 2019 con los números de teléfono personales de 5 trabajadores para cuestiones relacionadas con la formación de estos trabajadores, puede justificarse en alguna de las examinadas bases de legitimación. A este respecto manifiesta la parte reclamada que los trabajadores se muestran conformes con los canales de comunicación establecidos, participando en ellos, y que los nombres de las personas que firman la reclamación no coinciden con los nombres

de los integrantes del chat, de ahí que en este caso proceda traer a colación la doctrina de la Audiencia Nacional sentada, ente otras, en las SAN de 13 de junio de 2017 y SAN de 26 de junio de 2020, que considera necesario para poder apreciar la existencia de una infracción por falta de consentimiento que sea el propio afectado el que niegue su existencia, al ser el consentimiento personal e individual. Por tanto, no procede la imposición de una sanción por los hechos narrados por cuanto no se ha puesto de manifiesto por ninguno de los integrantes del chat la ausencia de consentimiento.

Contrariamente sí debe declararse incumplido el principio que consagra el art. 5.1.f) del RGPD con la remisión por la parte reclamada de dos correos electrónicos sin utilizar la opción de copia oculta revelando la dirección de correo del reclamante al resto de destinatarios sin su consentimiento y sin que resulte aplicable otra base de legitimación del art. 6 RGPD.

En consecuencia, teniendo en cuenta las consideraciones expuestas no puede concluirse que la entidad reclamada contara con una base de legitimación que amparara la revelación de la dirección de correo personal del reclamante. Por ello, esta Agencia considera que facilitar datos personales a terceros, dirección de correo electrónico, sin base de legitimación supone una vulneración de la confidencialidad que contraviene el principio de integridad y confidencialidad recogido en el artículo 5.1. f) del RGPD.

Así las cosas, la entidad reclamada al enviar el correo electrónico sin utilizar la opción CCO ha infringido el artículo 5.1. f) del RGPD,

IV

Tipificación y calificación de la infracción del artículo 5.1 f) del RGPD

Los principios relativos al tratamiento de datos de carácter personal se regulan en el artículo 5 del RGPD donde se establece que "los datos personales serán:

"a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

La infracción del artículo 5.1 f) del RGPD puede ser sancionada con multa de 20 000 000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5 a) del RGPD, que recoge como infracción “el incumplimiento de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5,6,7 y 9”.

El artículo 72.1 a) de la LOPDGDD señala que “en función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679”.*

V

Sobre la infracción del artículo 32 del RGPD

Tal y como se destacaba en el fundamento de derecho II la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

El examen de la documentación obrante en el expediente no permite apreciar un comportamiento diligente por parte del reclamado, que remitió dos comunicaciones a una pluralidad de destinatarios sin ocultar las direcciones

La reclamada no ha podido justificar que existieran medidas de seguridad adecuadas para garantizar la confidencialidad de los datos en los envíos por correo.

Además, al remitir la entidad reclamada comunicaciones al correo personal de los trabajadores sin utilizar la copia oculta, implica que las medidas de seguridad de la entidad reclamada no son adecuadas a la normativa de protección de datos.

De conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos constituyen una infracción, imputable al reclamado, por vulneración del artículo 32 del RGPD.

VI

Tipificación y calificación de la infracción del artículo 32 del RGPD

La seguridad en el tratamiento de datos personales viene regulada en el artículo 32 del RGPD donde se establece lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

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

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son

objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.
Sobre este particular, debe tenerse en cuenta que existen en el mercado herramientas que disminuyen el riesgo de realizar por error envíos de correos electrónicos a varios destinatarios sin emplear la opción de copia oculta, al mantener, por defecto, a los destinatarios ocultos.

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

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

En el caso que nos ocupa, el reclamado, al remitir un correo electrónico sin utilizar la opción de copia oculta está incumpliendo su obligación de aplicar las medidas técnicas
y organizativas apropiadas para garantizar un nivel de seguridad adecuado en el tratamiento de los datos personales recogido en el artículo 32 RGPD, sobre todo si se tiene en cuenta que existen en el mercado herramientas que disminuyen el riesgo de que se envíen por error correos electrónicos a varios destinatarios sin emplear la opción de copia oculta.

El artículo 83.4 del RGPD establece que se sancionarán con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía cuando se vulneren:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;*

El artículo 73 de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves a efectos de prescripción" dispone:

"En función del artículo 83.4 del Reglamento (UE) 2016/679 se considerarán graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel, y en particular los siguientes:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.">>

III
Principio de culpabilidad

El recurrente afirma que la resolución sancionadora habría vulnerado el principio de culpabilidad. Conforme al mismo, (artículo 28 Ley 40/2015) el Derecho Administrativo sancionador, en efecto, impone la obligación de que las conductas que sean sancionadas respondan a alguno de los dos criterios de imputación, o bien a título de dolo, o bien, a título de culpa.

Los factores que el recurrente aporta en su apoyo para negar la concurrencia de este principio serían los siguientes:

- Sólo se aportan dos correos electrónicos que implica sólo a un reducido grupo de trabajadores, aparentemente 40.

- En ningún momento el envío de dichos dos correos es realizado conscientemente con el ánimo de vulnerar los derechos, ni tampoco de forma negligente, claramente culposa, sino con el objetivo de informar a todos los trabajadores a la vez y de que todos supieran que los demás sabían lo mismo, al modo de un tablón de anuncios.

- El reclamado, en cuanto tuvo conocimiento de las imputaciones a través del requerimiento (E/00631/2021) de 02/02/2021, con el fin de evitar que se produjeran incidencias similares, ILUNION SEGURIDAD, S.A .tomó la decisión de adoptar la medida consistente en remitir un comunicado a todos sus mandos intermedios a fin de recordar que en ILUNION SEGURIDAD, S.A., están prohibidas tanto la creación de grupos de Whatsapp con los números de teléfono particular de los trabajadores como la remisión de correos sin emplear la opción de copia oculta (CCO) a las direcciones de correo electrónico particular de dichos trabajadores.

Pues bien, ninguno de ellos acreditaría la supuesta falta de culpabilidad. El primero se refiere únicamente al escaso número de correos electrónicos enviados, lo que como máximo podría ser tenido en cuenta para la fijación de la cuantía de la sanción, pero nunca para descarta la existencia de culpabilidad.

El segundo se refiere la presunta inexistencia de un "ánimo de vulnerar derechos". Esto último descartaría, en caso de confirmarse, la concurrencia del dolo en la acción, pero nunca de la negligencia.

Finalmente, las medidas adoptadas con posterioridad a la apertura del expediente (tercer factor alegado) obviamente no pueden eximir de culpabilidad en unos hechos producidos con anterioridad.

Como el propio recurrente indica, para apreciar la concurrencia del principio de culpabilidad, deberá constatarse que ha incurrido dolo o negligencia en la comisión de la infracción. En este caso, en la resolución sancionadora se motiva suficientemente la inexistencia de medidas de seguridad que impidieran que la pérdida de confidencialidad de los datos personales se hubiera producido. A este respecto, la única medida invocada en este recurso se refiere a un momento posterior a los hechos. En efecto, el recurrente afirma que “en cuanto tuvo conocimiento de las imputaciones” se transmitió la instrucción de no crear grupos de Whatsapp con números de teléfonos particulares, ni enviar correos electrónicos sin el uso de la funcionalidad “CCO”.

Por todo ello, no puede descartarse la concurrencia del principio de culpabilidad, sino todo lo contrario, esto es, la falta de medidas suficientes permitió que la pérdida de confidencialidad se produjera.

IV
Posible concurrencia de infracciones

A este respecto, el recurrente invoca la posibilidad de un proscrito “non bis in idem”, o subsidiariamente, la existencia de un concurso medial de infracciones entre las imputadas en el expediente, es decir, las vulneraciones de los artículos. 5.1.f) y. 32 del RGPD.

A este respecto debe indicarse lo siguiente:

Non bis in idem.

Las infracciones en materia de protección de datos están tipificadas en los apartados 4, 5 y 6 del artículo 83 del RGPD. Es una tipificación por remisión, admitida plenamente por nuestro Tribunal Constitucional. En este sentido, también el artículo 71 de la LOPDGDD realiza una referencia a las mismas al señalar que “*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*”.

En este sentido, el Dictamen del Consejo de Estado de 26 de octubre de 2017 relativo al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal dispone que “*El Reglamento Europeo sí tipifica, por más que lo haga en un sentido genérico, las conductas constitutivas de infracción: en efecto, los apartados 4, 5 y 6 de su artículo 83 arriba transcritos contienen un catálogo de infracciones por vulneración de los preceptos de la norma europea que en tales apartados se indican. El artículo 72 del Anteproyecto asume, no en vano, la existencia de dicho catálogo, cuando dispone que "constituyen infracciones los actos y conductas que supongan una vulneración del contenido de los apartados 4, 5 y 6 del Reglamento Europeo y de la presente ley orgánica".*

Las infracciones fijadas en los artículos 72, 73 y 74 del LOPDGDD lo son sólo a los efectos de la prescripción, tal y como reza el inicio de todos y cada uno de estos preceptos. Esta necesidad surgió en nuestro Estado dado que no existe en el RGPD referencia alguna a la prescripción relativa a las infracciones, dado que este instituto jurídico no es propio de todos los Estados miembros de la UE.

Debemos partir de que el RGPD es una norma jurídica directamente aplicable, que ha sido desarrollada por la LOPDGDD, sólo en aquello que le permite el primero. Así queda patente y en cuanto a la prescripción en la propia exposición de motivos de la LOPDGDD cuando expresa que *"La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona".*

Resulta de la aplicación e interpretación del RGPD, y no de la LOPDGDD, el que determina la gravedad de una infracción atendiendo a una serie de condicionantes previstos en el mismo.

Como podemos comprobar, no está presente en el RGPD una tipificación en infracciones muy graves, graves o leves típica del ordenamiento jurídico español, ni tampoco puede deducirse de su dicción que la vulneración de los preceptos del artículo 83.4 del RGPD correspondan a infracciones leves y los preceptos del artículo 83.5 o del artículo 83.6 del RGPD correspondan a infracciones graves.

Así, el considerando 148 habla de infracciones graves en contraposición con las leves cuando determina que *"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante.".*

Por todo ello, la gravedad de una infracción se determina a los efectos del RGPD y con los elementos dotados por éste.

Así, la clasificación de las infracciones a los efectos de la prescripción de la LOPDGDD no tiene virtualidad en cuanto a la determinación de la gravedad de la infracción a los efectos del RGPD ni respecto de la imposición de las multas correspondientes, en su caso.

A título meramente ilustrativo indicaremos que, una misma conducta, como por ejemplo la falta información en la política de privacidad de una empresa, pueda ser considerada grave o leve a los efectos del Reglamento (en atención a las circunstancias citadas en el considerando 148 en relación con las previsiones del artículo 83 del RGPD, pues no es lo mismo el incumplimiento por una empresa multinacional que por un autónomo) y en ambos casos con prescripción leve. La gravedad de una infracción determinará su sanción.

Como ha concluido el Consejo de Estado, el modelo europeo de sanciones en el RGPD comporta un amplio arco en el importe de la sanción, en función de la concurrencia de las circunstancias del art. 83.2, las cuales son objetivas y comprobables por los tribunales. De hecho, y como resulta de la propia STC 150/2020, de 22 de octubre, lo que se considera contrario al principio de taxatividad y lex certa, la vertiente material del art. 25 CE, es:

encomendar por entero tal correspondencia a la discrecionalidad judicial o administrativa, «ya que ello equivaldría a una simple habilitación en blanco a la administración por norma legal vacía de contenido material propio»

En el RGPD, norma que establece las infracciones y sanciones, no concurre dicha circunstancia no deseada por el TC, como es encomendar "por entero" (sic) a la discrecionalidad administrativa la correspondencia entre infracción y sanción. Bien al contrario. Ya el art. 83.4 RGPD y 83.5 RGPD establecen una primera distinción en cuanto al importe de las sanciones a imponer según los preceptos infringidos. El art. 83.6 RGPD, por otra parte, también acota debidamente la infracción. El art. 83.2 RGPD, por otro lado, contiene las circunstancias que el legislador europeo considera que las autoridades de control han de tener en cuenta para determinar el importe de la sanción, que son circunstancias que no dependen de la "discrecionalidad administrativa", sino de una apreciación objetiva, y revisable por los tribunales.

Por último, cabe mencionar que la doctrina constitucional (por todas STC 150/2020) se dirige sólo a aquellas normas en las que el propio legislador ha establecido la categorización de las infracciones en tres categorías (leves, graves o muy graves). Este no es el caso. Y no parece que de la Constitución resulte de manera inexorable que el legislador deba siempre dividir las infracciones en leves/graves/muy graves. Lo que el TC proclama es que el administrado pueda prever la correspondencia entre la conducta infractora y la posible sanción, lo que sin duda aquí se da, pues el RGPD determina las conductas infractoras, y las posibles sanciones, sin que pueda existir, por otra parte, tacha de "inconstitucionalidad" en un "Reglamento" europeo, que por virtud del principio de efecto directo, (sentencia Van Gend en Loos) y de primacía (sentencia Costa v ENEL) desplaza a toda normativa estatal, incluso a la de rango constitucional, como es sabido (Sentencia Costa v ENEL: *los objetivos de los Tratados se verían socavados si el Derecho de la Unión pudiera subordinarse al Derecho interno*).

Pues bien, como se desprende del fundamento anterior existe diferencia entre la vulneración del art. 5.1.f y el artículo 32 del RGPD.La diferente tipificación en apartados incluso distintos del art. 83 del RGPD y la diferente calificación de ambos a los efectos de la prescripción en la LOPDGDD, así lo corrobora.

El art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales, lo que puede producirse o no por ausencia o deficiencia de las medidas de seguridad.

Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita *"mediante la aplicación de medidas técnicas y organizativas apropiadas",* que no son estrictamente de seguridad.

Como hemos señalado anteriormente, cuando el art. 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD lo

hace en el sentido previsto en el art. 25 del RGPD relativo a la privacidad desde el diseño.

Este precepto determina que,

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

Reiteramos que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el art. 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. De seguridad. Sólo de seguridad.

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo mientras que en el caso del artículo 5.1.f) del RGPD se debe garantizar la confidencialidad e integridad. Como se puede observar los dos artículos persiguen fines distintos, aunque puedan estar relacionados.

Pues bien, no se ha vulnerado el principio non bis in idem, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una brecha de seguridad, la infracción del art. 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y disponibilidad, la infracción del art. 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad). De hecho, si las medidas de seguridad se hubieran detectado en este procedimiento por la AEPD sin que se hubiera producido la pérdida de confidencialidad y de disponibilidad, únicamente hubiera sido sancionada por el art. 32 del RGPD.

Y todo ello frente a las alegaciones formuladas de contrario que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el art. 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de disponibilidad y confidencialidad, únicamente, y mediante el art. 32 del RGPD la ausencia y deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes, añadimos, que infringen el RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad y de disponibilidad.

Concurso medial

En primer lugar, significar que aunque ambas infracciones están tipificadas en el art. 83.5 del RGPD, no hay una supuestamente más grave y otra supuestamente más leve.

Segundo, que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD.

1. El RGPD es un sistema cerrado y completo.

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

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

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

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

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

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

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

Sigue indicando el considerando 13 del RGPED que,

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

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

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

De esta forma las medidas correctivas, que son todas las previstas en el art. 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.

Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

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

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

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

minuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

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

2. No hay laguna legal, no hay aplicación supletoria del art. 29 de la LRJSP

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

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

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

En tercer lugar y ya deteniéndonos en el supuesto concreto examinado, se debe destacar que no hay concurso medial.

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

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

Los hechos constados determinan la comisión de dos infracciones distintas, sin que la conculcación del artículo 32 del RGPD, tal y como asevera la parte recurrente, sea el medio necesario por el que se produce la infracción del artículo 5.1.f) del RGPD (vulneración del principio de confidencialidad).

V
Proporcionalidad de la sanción

El recurrente afirma que la cuantía de las sanciones impuestas sería desproporcionada. A este respecto se basa únicamente en la importante reducción de la cuantía que se efectuó por parte de esta Agencia entre la propuesta de resolución y la resolución. En efecto, mientras que en aquella se proponía la imposición de sendas sanciones de 100.000€ (artículo 5.1.f) y 50.000€ (artículo 32), las finalmente impuestas fueron de 10.000€ y 5.000€ respectivamente.

Ello se debe, como explicita la resolución sancionadora, a dos motivos: por una parte, se descartó la comisión de infracción por la creación del grupo de Whatsapp; y por otra a que la infracción fue inicialmente considerada cometida a título de dolo, de manera intencionada, mientras que finalmente se consideró que únicamente se cometió de manera negligente. Ello permitió la reducción de la cuantía total en un importe de 135.000€ (al rebajarse de 150.000 a 15.000€).

Este argumento es utilizado a su favor ahora por el recurrente, indicando que la modificación del título de imputación (de dolo a culpa) le impidió alegar sobre esta última. Es evidente que este argumento no puede prosperar, ya que en todo momento procedimental el interesado tuvo oportunidad de alegar sobre este factor, que estaba ya recogido desde el propio acuerdo de inicio del expediente sancionador como agravante. De hecho, esto fue tenido en cuenta por esta Agencia para la importante reducción de la sanción (que quedó en un únicamente un 10% de la inicialmente propuesta) en la resolución sancionadora final.

Con ello, la posible intencionalidad de la infracción no ha sido tenida en cuenta como agravante de la culpabilidad (como sí se hacía en el acuerdo de inicio). Por su parte, la concurrencia de culpa en la infracción queda suficientemente explicada tanto en la propia resolución sancionadora como en los apartados anteriores de esta resolución.

Adicionalmente, en el recurso de reposición se alega que esta Agencia no habría tenido en cuenta diversas circunstancias, previstas legalmente, y que, a juicio de la recurrente, acarrearían la disminución de la cuantía:

- Art. 83.2.a) RGPD:

    - La falta de gravedad y mínima duración de la supuesta infracción: se trataría de 2 correos electrónicos muy cercanos en el tiempo y dirigidos ambos a los mismos destinatarios

      La existencia de dos correos y además ambos dirigidos a múltiples destinatarios, impide considerar esta circunstancia como atenuante. Debe aclararse, por lo demás, que tampoco se ha considerado como agravante.

    - La naturaleza, alcance o propósito de la operación de tratamiento de que se trate: el objeto del tratamiento era informar a los trabajadores de cuestiones COVID (salud pública). Del mismo modo que lo anterior, la comisión de la infracción sin haber tenido consentimiento de los afectados es de tal naturaleza que impide considerar esta circunstancia como atenuante. Al igual que la circunstancia anterior, tampoco se ha considerado agravante.

    - El número de interesados afectados: los correos electrónicos a un total de 41 (casi la totalidad estarían duplicados);

No puede considerarse que haber afectado a múltiples personas, en este caso 41, pueda ser considerado como atenuante. Se trata de un elevado número de personas que vieron comprometidos sus datos.

- El nivel de los daños y perjuicios que hayan sufrido: no se tiene constancia, afirma la recurrente, que la supuesta vulneración haya supuesto ningún daño o perjuicio para ningún trabajador.

  Si bien la producción de daños y perjuicios podría haber sido considerada como agravante, la operación no puede efectuarse en sentido contrario, de modo que rebajara la cuantía de la sanción

- Art. 83.2.b) RGPD: no habría habido intencionalidad ni negligencia alguna en la infracción. A este respecto, en caso de no haber existido ni intencionalidad ni negligencia, no habría podido imputarse la infracción, ya que la normativa exige la concurrencia de una de las dos. De hecho, en la resolución recurrida se explicitan los motivos por los que se considera que existe negligencia:

  "El examen de la documentación obrante en el expediente no permite apreciar un comportamiento diligente por parte del reclamado, que remitió dos comunicaciones a una pluralidad de destinatarios sin ocultar las direcciones La reclamada no ha podido justificar que existieran medidas de seguridad adecuadas para garantizar la confidencialidad de los datos en los envíos por correo.

  Además, al remitir la entidad reclamada comunicaciones al correo personal de los trabajadores sin utilizar la copia oculta, implica que las medidas de seguridad de la entidad reclamada no son adecuadas a la normativa de protección de datos."

- Art. 83.2.c) y f) RGPD: Medidas tomadas. La recurrente habría tomado la decisión, tras conocer este caso, de "*adoptar la medida consistente en remitir un comunicado a todos sus mandos intermedios a fin de recordar que en ILUNION SEGURIDAD, S.A. están prohibidas tanto la creación de grupos de Whatsapp con los números de teléfono particular de los trabajadores como la remisión de correos sin emplear la opción de copia oculta (CCO) a las direcciones de correo electrónico particular de dichos trabajadores*"

  Si bien se valora positivamente la adopción de medidas reactivas para evitar futuros incumplimientos, el hecho de haber sido adoptadas tras conocer la reclamación hace que impida ser considerada como atenuante.

- Art. 83.2.e) RGPD: infracciones anteriores cometidas por el responsable: ILUNION SEGURIDAD, S.A., no habría sido anteriormente sancionado por incumplir la legislación en materia de protección de datos

Esta circunstancia solo puede ser tenida como agravante en caso de concurrir la existencia de infracciones anteriores. La Sentencia de la Audiencia Nacional, de 5 de mayo de 2021, rec. 1437/2020, indica que "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento*". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante.

- Art. 83.2.g) RGPD: categorías de los datos de carácter personal afectados por la infracción: los datos supuestamente comprometidos son únicamente la dirección de correo electrónico, datos que no tienen la consideración, conforme afirma la recurrente, de datos especialmente protegidos.

  Esta circunstancia no puede considerarse como atenuante. Hay que tener en cuenta que datos como la dirección de correo electrónico son utilizados para la producción de determinados fraudes, como el *phishing* o la suplantación de personalidad.

- Art. 83.2.k) RGPD: beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción: ni se habrían obtenido beneficios ni se evitado pérdidas, ya que, indica la recurrente, en ningún caso la supuesta infracción habría tenido intención alguna.

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

En relación con los precedentes mencionados por el recurrente, cabe afirmar lo siguiente: en primer lugar, debe tenerse en cuenta, conforme se establece en el artículo 83 del RGPD , el volumen de negocio de la entidad sancionada. Siendo así que conforme se declara en la resolución recurrida, el correspondiente al interesado es de 185 millones de euros.

Adicionalmente, como ha declarado muy reiteradamente nuestra jurisprudencia, no existe un supuesto derecho a la "igualdad en la ilegalidad", siendo así que la resolución motiva las circunstancias en que se basa para la determinación de la cuantía.

Por lo demás, resta únicamente decir que para las infracciones del artículo 5.1.f) el RGPD prevé sanciones máximas de 20 millones de euros, mientras que para las del artículo 32 el máximo sería de 10 millones. Con ello, las cuantías impuestas se sitúan clarísimamente dentro de grado mínimo de lo legalmente previsto.

V
Conclusión

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

VI
Resolución extemporánea

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

De acuerdo con lo establecido en el art. 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

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

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

Vistos los preceptos citados y demás de general aplicación,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ***ILUNION SEGURIDAD, S.A.*** contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 14 de febrero de 2023, en el expediente RR/00162/2023.

SEGUNDO: NOTIFICAR la presente resolución a ***ILUNION SEGURIDAD, S.A.***.

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

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

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

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

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

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

180-111122

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