Expediente N.º: PS/00452/2022

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 16 de diciembre de 2020, tuvo entrada en esta Agencia Española de Protección de Datos (en adelante AEPD) escrito de reclamación, presentado por ***A.A.A.*** contra ***ILUNION SEGURIDAD, S.A.*** con NIF ***A78917465.***

En particular por las siguientes circunstancias:

La parte reclamante manifestó en la reclamación inicial presentada que se enviaron comunicaciones laborales a los teléfonos particulares sin haber prestado su consentimiento ni contar con la participación de la representación de los trabajadores, y que se han revelado las direcciones de correo electrónico personales de los trabajadores al enviar correos electrónicos sin utilizar la opción de envío con copia oculta a todos los destinatarios del correo electrónico.

Junto a su reclamación la parte reclamante aporta copia de dos correos electrónicos remitidos a varios destinatarios sin utilizar la opción de copia oculta, así como copia de los mensajes instantáneos de la aplicación WhatsApp recibidos por la parte reclamante y otros trabajadores y remitidos por la empresa en la que prestan sus servicios.

Finalmente, la parte reclamante alega en su reclamación inicial que en ningún momento ha dado su consentimiento para ser incluido en grupos de comunicación de mensajería instantánea de la aplicación WhatsApp creados por la coordinación del servicio del aeropuerto de Fuerteventura, ni para recibir correos electrónicos de carácter laboral sin que sea utilizada la opción de copia oculta de los remitentes habiéndose dado a conocer al resto de trabajadores su dirección de correo electrónico sin su consentimiento.

SEGUNDO: De acuerdo con el mecanismo previo a la admisión a trámite de las reclamaciones que se formulan ante la AEPD, previsto en el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD), que consiste en dar traslado de las mismas a los Delegados de Protección de Datos designados por los responsables o encargados del tratamiento, o a éstos cuando no los hubieren designado, y con la finalidad señalada en el referido artículo, se dio traslado de la reclamación a ILUNION SEGURIDAD, S.A. (en adelante, la parte reclamada) para que procediera a su análisis y diera respuesta en el plazo de un mes, lo que verificó mediante escrito de fecha de entrada en esta Agencia de 4 de marzo de 2021.

TERCERO: En fecha 15 de abril de 2021, tras analizarse la documentación que obraba en el expediente, se dictó resolución por la directora de la Agencia Española de Protección de Datos, acordando el archivo de la reclamación.

La resolución fue notificada a la parte reclamante, en fecha 15 de abril de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada según certificado que figura en el expediente.

CUARTO: En fecha 22 de abril de 2021, la parte reclamante interpone un recurso potestativo de reposición (RR/00267/2021) a través del Registro Electrónico de la AEPD, contra la resolución recaída en las actuaciones E/00631/2021, en el que muestra su disconformidad con la resolución impugnada, argumentando que el hecho de no haber mostrado disconformidad al tratamiento de datos personales no habilita a la parte reclamada a utilizar los datos personales como correo electrónico o número de teléfono particular, no corporativo, para las comunicaciones realizadas.

Asimismo, añade que las comunicaciones realizadas por el servicio de mensajería de WhatsApp no fueron con motivo de un ERTE, sino para la organización de turnos de trabajo comunicados fuera del horario laboral y el hecho de que los trabajadores realicen su trabajo en el exterior no implica que tengan que hacerse las comunicaciones a teléfonos móviles particulares ya que la parte reclamada cuenta con una oficina física en el centro de trabajo.

QUINTO: Analizadas las alegaciones de la parte reclamante del RR/00267/2021, el 30 de julio de 2021, la Directora de la Agencia Española de Protección de Datos resuelve estimar dicho recurso de reposición, generándose así la apertura del procedimiento sancionador PS/00456/2021, notificado al reclamado el 11 de noviembre de 2021.

SEXTO: A lo largo del procedimiento sancionador PS/00456/2021, la entidad reclamada alega la indefensión sufrida en el recurso de reposición (RR/00267/2021) interpuesto por el reclamante ante esta Agencia denunciando los hechos objeto del presente procedimiento, que dieron lugar a su estimación y correspondiente apertura del procedimiento sancionador PS/00456/2021.

La entidad reclamada, alega que no se le comunicó la interposición de dicho recurso potestativo de reposición interpuesto por el reclamante ante la Agencia, y que por tanto no pudo defenderse.

Así las cosas, de conformidad con el artículo 118 de la ley 39/2015 de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas (LPACAP), que regula el derecho de audiencia de los interesados, esta Agencia decide archivar el procedimiento sancionador PS/00456/2021 y retrotraer sus actuaciones al momento en que se omitió el trámite de audiencia en el recurso potestativo de reposición (RR/00267/2021), de conformidad con el artículo 119.2 de la LPACAP.

SEPTIMO: En fecha 15 de marzo de 2022 se remitió el recurso interpuesto a la parte reclamada en el marco de lo establecido en el artículo 118 de la LPACAP a los efectos de que formulase las alegaciones y presentase los documentos y justificantes que estimase procedentes. La notificación del trámite de audiencia se produjo en fecha 17 de marzo de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

OCTAVO: Con fecha 31 de marzo de 2022 la parte reclamada presenta alegaciones al recurso de reposición interpuesto, 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 "***GRUPO.1", 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.

NOVENO: Con fecha 8 de agosto de 2022, la Directora de la Agencia Española de Protección de Datos, estima el recurso de reposición interpuesto por ***A.A.A.*** contra la resolución de esta Agencia dictada en fecha 15 de abril de 2021, por la que se acordaba el archivo de la reclamación referida a ***ILUNION SEGURIDAD, S.A.***

DÉCIMO: Con fecha 20 de septiembre de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD.

UNDÉCIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la LPACAP, la parte reclamada presentó escrito de alegaciones en el que reitera que las comunicaciones a través de WhatsApp o correo electrónico son utilizadas únicamente para cuestiones relativas a la relación laboral, esto es, para la formación, bajas, información COVID, determinación de turnos derivados del ERTE COVID, días de libranza, etc., y a veces puede resultar necesario que la información sea compartida entre varios trabajadores, a fin de que todos ellos conozcan que los demás están informados de lo mismo, y resolver dudas generales.

La entidad reclamada insiste en que WhatsApp en ningún momento es utilizado para dar instrucciones diarias de trabajo, encargar tareas, etc., señalando además que la información que se comparte, de no ser canalizada a través del teléfono o el correo electrónico, hubiera tenido que ser enviada por carta postal al domicilio de cada trabajador, medio absolutamente ineficiente.

Asimismo, argumenta que los trabajadores se muestran conformes con los canales de comunicación así establecidos, participando en ellos, o incluso iniciándolos ellos mismos, lo que es prueba de un comportamiento activo en aceptar que se utilicen sus datos de contacto (número de teléfono, correo, etc.) a tal efecto.

Explica la entidad que los mensajes de WhatsApp se hacen más frecuentes a partir de marzo de 2020, así como los correos electrónicos aportados, siendo muchas de dichas comunicaciones de temática COVID, en cuanto se refieren tanto a medidas preventivas, al ERTE, como a protocolos establecidos por el Aeropuerto. Los comunicados por WhatsApp y correo electrónico son casi en su totalidad derivados de la situación de ERTE de fuerza mayor, por la bajada del número de viajeros en el Aeropuerto, originada por la pandemia COVID.

Declara que no existe constancia de que la coordinadora haya creado un grupo de WhatsApp con los teléfonos particulares de 5 trabajadores, pues de las pruebas aportadas por el reclamante se desprende que participan en el chat personas, de las

que en un principio ninguna de ellas es el denunciante. Los supuestos trabajadores integrantes del grupo (5 personas) tampoco quedan identificados por lo que se desconoce si son o no trabajadores de la empresa, y si la supuesta coordinadora contó o no con el consentimiento de los mismos para crear el grupo, esto es, para compartir los números de teléfono entre todos sus componentes. A este respecto, resulta muy revelador que ni siquiera coinciden los nombres de las personas que integran dicho chat con las personas que firman la reclamación junto con el reclamante.

.

En cuanto a la parte reclamante, la reclamada especifica que resulta claro el consentimiento del trabajador en tratar el dato de su número de teléfono móvil para tratarlo a través de WhatsApp con la finalidad de tratar aspectos relacionados con su relación laboral, y que éste ni mostró su disconformidad con el tratamiento de sus datos personales, ni ejercitó en ningún momento ante ILUNION SEGURIDAD, S.A., los derechos que le asisten de conformidad con el RGPD. Tampoco hubo trabajadores que ejercieran sus derechos durante el tiempo en que fue utilizada dicha plataforma de mensajería ni que bloquearan el chat.

Indica que este tratamiento también puede quedar amparado en la necesidad del mismo para la ejecución de un contrato laboral en el que el interesado es parte y, subsidiariamente, en la necesidad de dicho tratamiento para la satisfacción de intereses
legítimos perseguidos por ILUNION SEGURIDAD, S.A., de conformidad con lo dispuesto en el artículo 6.1.b) y f) del RGPD. En este orden de ideas cita en su defensa la resolución R/00026/2021 de la AEPD y la SAN 2087/2020, de 29 de julio.

Afirma de nuevo que 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, 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.

DÉCIMO SEGUNDO: Con fecha 6 de octubre de 2022, el instructor del procedimiento acordó dar por reproducidos a efectos probatorios la reclamación interpuesta por ***A.A.A.*** y su documentación, así como los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación.

Asimismo, se dan por reproducidas a efectos probatorios las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por ***ILUNION SEGURIDAD, S.A.***, y la documentación que a ellas acompaña.

DÉCIMO TERCERO: Con fecha 8 de noviembre de 2022 se formuló propuesta de resolución, proponiendo lo siguiente:

Que por la Directora de la Agencia Española de Protección de Datos se sancione a ***ILUNION SEGURIDAD, S.A.***, con NIF ***A78917465***, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, con una sanción de 100.000 € (cien mil euros).

Que por la Directora de la Agencia Española de Protección de Datos se sancione a ***ILUNION SEGURIDAD, S.A.***, con NIF ***A78917465***, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD una sanción de 50.000 € (cincuenta mil euros).

DÉCIMO CUARTO: de acuerdo con el informe recogido de la herramienta AXESOR, la entidad ILUNION SEGURIDAD, S.A. es una gran empresa, constituida en el año 1988, con un volumen de negocios de ******CANTIDAD.1*** € en el año 2021.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: 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.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II
Brecha de seguridad

Establece el artículo 4.12 del RGPD que se considera "*violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione 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*."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad.

Hay que señalar que 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.

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 Don Eleuterio (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 "***GRUPO.1" 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.”*

VII
De los poderes de la Autoridades de control

El artículo 58.2 del RGPD dispone lo siguiente: “Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

VIII
Sanción

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD.

Por tanto, procede graduar la sanción a imponer de acuerdo con los criterios que establece el artículo 83.2 del RGPD, y con lo dispuesto en el artículo 76 de la LOPDGDD, respecto al apartado k) del citado artículo 83.2 RGPD.

El artículo 83.2 del RGPD establece 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).

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;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

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;

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;

g) las categorías de los datos de carácter personal afectados por la infracción;

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 medida;

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 el presente caso, esta Agencia mantiene como agravante la circunstancia contemplada en el artículo 83.2 b) del RGPD, la intencionalidad o negligencia en la infracción, si bien no considera en este caso la existencia de intencionalidad sino de una clara falta de diligencia de la entidad reclamada.

El balance de tal circunstancia recogida en el artículo 83.2.b) del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en su artículo 5.1.f), permite fijar una sanción de 10.000 euros (diez mil euros) y con respecto a la infracción cometida al vulnerar lo establecido en su artículo 32 RGPD, permite fijar una sanción de 5.000 euros, (cinco mil euros).

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

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

PRIMERO: IMPONER a ***ILUNION SEGURIDAD, S.A.***, con NIF ***A78917465***,

- 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).

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

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 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, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. 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 LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo.

De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

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