Expediente Nº: E/03736/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***PROSEGUR ESPAÑA SL*** en virtud de denuncia presentada por D. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 17 de abril de 2015, tuvo entrada en esta Agencia escrito de D./Dña. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia que, es empleado de la empresa PROSEGUR ESPAÑA SL, (en lo sucesivo PROSEGUR) y que por medio de uno de sus mandos intermedios, en particular el Coordinador de Operaciones en Madrid, se comunica todo lo concerniente al servicio mediante el envío de e-mails a todos los Vigilantes de Seguridad a su cargo. Indica que lo expuesto no constituiría ninguna vulneración en materia de Protección de Datos, si las comunicaciones se hicieran con "Copia Oculta", pero los e-mails se envían de manera que todos los trabajadores destinatarios aparecen con nombre y apellidos en los mismos. También se comunica por e-mail a TODOS los Vigilantes de Seguridad, estén interesados o no, los juicios que tienen señalados para asistir como testigos de hurtos, etc. En los mismos aparecen los nombres y apellidos, así como el lugar y la fecha, poniendo en riesgo de esta manera la integridad física de los mismos, al poder acceder a esos datos cualquier persona interesada en esos juicios del orden jurisdiccional penal.

Indica que los datos que han sido cedidos son los siguientes:

-Nombres y apellidos.

-Direcciones de correos electrónicos.

-Número del documento nacional de identidad (DNIs) o (NIEs)

-Número de Teléfono particular, privado

-lugar de residencia

-Número de orden de Empleado

-Horario y lugar de trabajo de todo el personal y las zonas

-Bajas, incorporaciones, sucesos de personas concretas

-Informaciones relativas a infracciones penales

Resalta que en su caso como en el de otros, además dichos datos "*conforman un perfil de una persona física identificada y identificable, hacen referencia de manera indirecta al origen racial incluso religión o creencias".*

Aporta impresión de múltiples correos electrónicos dirigidos a su cuenta de gmail en los que se aprecia visible la lista de direcciones de correo electrónico de otros destinatarios.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados:

A) Del análisis de los correos electrónicos aportados por el denunciante se desprende

lo siguiente:

1. Los temas que tratan los correos son muy diversos, desde una información de la entrada en vigor de la autorización para usar ropa de verano, remitida sin copia oculta a unos cien destinatarios, a tablas con las horas denominadas “faltantes de jornada” de empleados identificados con nombre y apellidos y un código que puede ser el de empleado.

   También hay correos informando de los turnos y los lugares donde se deben desempeñar, así como cursos incluyendo una tabla de asistentes en la que se indica el nombre y apellidos de unas 90 empleados y su número de DNI.

   Existen también correos electrónicos que contienen tablas con las citaciones como testigos de los vigilantes en las que se especifica en cada caso el nombre del citado, la tienda donde se encontraba trabajando cuando ocurrieron los hechos, con fecha, hora y juzgado de citación así como número de referencia del atestado y del procedimiento judicial.

   En los correos donde se informa de las sustituciones de compañeros se informa en ocasiones de la zona (Coslada, Valdeavero) donde vive el sustituto. También se comentan las nuevas incorporaciones.

2. El correo electrónico **más antiguo es de fecha** 19 de abril de 2014 **y el más moderno de** 21 de marzo de 2015.

3. No se observan datos de salud, origen racial, afiliación, religión o creencias. El denunciante debe referirse a suposiciones que se podrían realizar a partir de los nombres (extranjeros) de las personas.

B) Al objeto de aclarar los hechos denunciados se ha solicitado a PROSEGUR la siguiente información y documentación:

1. **Origen de las direcciones de correo** electrónico de los trabajadores, que se utilizan para la remisión de correos electrónicos tales como cuadrantes, cursos, etc y que, por sus dominios (yahoo, hootmail, gmail) no son correos corporativos sino al parecer correos personales.

   Motivo por el cual no se remiten los correos electrónicos con copia oculta al objeto de no desvelar las direcciones de correo de los trabajadores al resto de trabajadores.

   Acreditación documental del consentimiento otorgado por los trabajadores para el tratamiento de sus direcciones de correo personales, así como para su comunicación al resto de trabajadores.

2. Justificación existente para la difusión o comunicación:

2.1. de las horas de absentismo o a recuperar (“faltante de jornada”) de unos trabajadores a otros.
2.2. de los números de DNI de unos trabajadores a otros.
2.3. del lugar de residencia de unos trabajadores a otros.
2.4. de los “señalamientos” o citaciones judiciales con lugar fecha y hora exacta, de unos trabajadores a otros. (El denunciante indica al respecto que supone una falta de seguridad con riesgo para la integridad física de los vigilantes dar

a conocer a otros o difundir sus ubicaciones con fechas y horas exactas de forma innecesaria).

Se pide en todos los casos información de la justificación existente, con documentación acreditativa de la habilitación legal ostentada para ello, en su caso.

Recibida contestación, los representantes de PROSEGUR ESPAÑA SL manifiestan lo siguiente:

"II.-Respecto a la primera de las cuestiones planteadas en el punto primero del Requerimiento, esto es, el ***origen de las direcciones de correo electrónico*** *de los empleados que se utilizan para la remisión de correos electrónicos con fines laborales, indicar que han sido facilitados por los propios empleados. En relación a este punto, se aporta […] el correo electrónico remitido por el Sr.* ***A.A.A.****, en virtud del cual queda acreditado que él mismo facilita su dirección de correo electrónico al coordinador del servicio, […] consintiendo su tratamiento.*

Con carácter general, a los vigilantes de seguridad no se les asigna una dirección de correo corporativo, ya que al trabajar en las oficinas del cliente no lo utilizan más que para comunicarse con su coordinador en caso de que tengan un asunto personal que afecte al servicio o recibir instrucciones en relación al servicio. Si se le facilitase una dirección de correo electrónico con dominio de Prosegur, por temas de seguridad, debería asignársele también un teléfono móvil, medida que se hace impracticable dado el elevado número de vigilantes que forman parte de la plantilla de Prosegur.

Por todo lo anterior, se solicita a los vigilantes de seguridad que faciliten una dirección de correo electrónico, contratada con el proveedor que elijan, para comunicarse con Prosegur con la recomendación de que habiliten la misma exclusivamente para este fin. No obstante, se escapa del control de esta parte si utiliza la dirección de correo facilitada con más fines, como si se tratase de un correo personal, o únicamente para comunicarse con su coordinador.

III.- En relación con la segunda cuestión del apartado primero, ***el motivo por el cual no se remiten los correos electrónicos con copia oculta****, es exclusivamente porque resulta imprescindible que todas las personas afectadas por un servicio se conozcan entre ellas. También es necesario que los trabajadores afectos a un servicio sean informados conjuntamente del cuadrante, de un cambio de turno, de una baja de un compañero, de un curso al que tienen que asistir, etc., de forma que puedan coordinarse entre ellos. Si se realizasen las comunicaciones por separado, sin informar a un vigilante de lo que van a realizar sus compañeros, probablemente faltaría información y el servicio no podría prestarse con normalidad.*

También podría ocurrir que al coordinador se le olvide incluir una persona -dado el elevado número de personas afectadas por el servicio-, o que por error no cuadre la información en su conjunto, etc. Por todo ello, es primordial que todos y cada uno de los vigilantes de seguridad sepan a quien se ha remitido la información, para que en caso de error pueda informar al coordinador para que tome las medidas que considere oportunas.

Como hemos apuntado anteriormente, se utiliza como vía de comunicación empleado/empresa, que puede incluir o no el nombre y apellidos del trabajador en cuestión-al igual que cualquier dirección de correo corporativo de Prosegur-; la única diferencia es el dominio. En cualquier caso, las direcciones de correo

electrónico se han utilizado siempre con el consentimiento de los trabajadores afectados, son ellos los que la facilitan de "motu proprio", y con la finalidad para la cual se recabaron: gestionar el servicio.

IV.- Respecto a la tercera cuestión del apartado primero, adjuntamos copia de las condiciones adicionales que firman los vigilantes de seguridad junto con el trabajo de contrato dónde se autoriza a Prosegur a tratar los datos de carácter personal de sus trabajadores que faciliten a lo largo de la relación laboral, […]

Respecto al consentimiento para comunicar su dirección de correo electrónica al resto de trabajadores, como hemos comentado antes, se trata de una cuenta de correo para cuestiones profesionales, habilitada y utilizada exclusivamente para coordinar el servicio y cumplir el objeto del contrato. Además, a estos efectos, los empleados de Prosegur, son Prosegur, y no cabe hacer distinción alguna entre ellos, por lo que no se ha producido una comunicación o cesión de datos en ese sentido. Otra cosa distinta es que los empleados de Prosegur utilizasen los datos fuera del ámbito de su actividad, en cuyo caso, se trataría de un tratamiento no consentido.

*Cuando el **Sr. A.A.A.** facilita su dirección de correo electrónico al coordinador, ya se le había informado acerca del uso que se le iba a dar, y prestó su consentimiento para ello. En este sentido, durante toda la relación laboral, se utilizó su cuenta de correo para remitir todas y cada de las comunicaciones -que recibe con copia a otros de sus compañeros- sin que en ningún momento haya manifestado su disconformidad, desde abril de 2014 hasta mayo de 2015 que finaliza su relación laboral con Prosegur.*

V.- En relación con el punto 2.1 del Requerimiento, son varias las razones para informar sobre las horas de absentismo o a recuperar de unos trabajadores a otros, entre ellas, por impulsar los valores de Prosegur, la transparencia y la igualdad. Todos deben recuperar las horas de absentismo sin hacer distinción alguna. Esta información la facilita el coordinador a los miembros del mismo equipo o centro, en su beneficio, para que puedan coordinarse entre ellos. El conocimiento de esas horas y su necesidad de recuperación permite que el grupo de personas asignado a un servicio a que conozca la razón por la que uno de los miembros del equipo asignado realiza o no más horas en un cuadrante. Con ello se trata de evitar que los miembros de ese equipo entiendan que se ha favorecido/perjudicado a alguna persona concreta. No obstante, esta información es totalmente deducible sumando las horas de los cursos y las ausencias por vacaciones que se hayan producido durante ese periodo, por lo que en ese correo únicamente se recoge información que ya es conocida por cada uno de los destinatarios del correo y que es la normal que surge en el marco de una relación laboral.

VI.- Respecto al punto 2.2 del Requerimiento, en la propia hoja de firmas para acreditar la asistencia al curso aparece el nombre y apellidos de cada trabajador que va a asistir al mismo junto con su número de DNI. A pesar de que se trata de un dato de carácter personal, es un dato cuya utilización es necesaria dentro del ámbito de la empresa, para identificar a los trabajadores que van a participar en el curso, o para cualquier otra finalidad, por ejemplo, incluirlo en un contrato o escrito o decidir si aceptar la recepción de un paquete, que manejan o conocen otras personas dentro del ámbito de la compañía, sin que ese conocimiento suponga una cesión ya que forman parte de la plantilla de Prosegur. Por

supuesto, si esa persona que maneja esos datos hace un uso desproporcionado o ilegítimo de ellos, no hay duda que le será imputable la comisión de una infracción de la normativa sobre protección de datos, pero mientras los utilice dentro del ámbito de la empresa supone un tratamiento más que justificado.

VIL- Respecto a la justificación del punto 2.3, se trata de los centros de trabajo o servicio al que van a estar asignados cada uno de los trabajadores, pero en el e-mail no indica que se trate de su lugar de residencia. Se trata de un ejercicio de transparencia y de coordinación, para que cada uno de ellos tenga conocimiento a qué centros van a estar asignados sus compañeros, y así gestionar de una manera más eficaz cualquier modificación que pueda surgir, y revisar y gestionar entre todo que los cuadrantes encajan. En cualquier caso, la información recogida en el e-mail no refleja el domicilio de ninguno de los trabajadores, sino se limita a indicar las poblaciones o barrios dentro de la Comunidad de Madrid dónde va a prestar los servicios cada uno de los vigilantes. ***Como en la anterior alegación se trata de un ejercicio más de transparencia****. Se busca que los miembros de un equipo conozcan el por qué se asigna o no un centro de trabajo concreto (se procura, en la medida de los posible, evitar que el trabajador se desplazase lejos de su zona de residencia).*

VIII.- En relación con el punto 2.4 del Requerimiento, es imprescindible que los compañeros conozcan la fecha y hora a las que los compañeros citados no van a poder asistir al trabajo. Si por ejemplo un trabajador está citado en Móstoles a primera hora de la mañana, es probable que pueda llegar a prestar el servicio a mediodía si su centro asignado está en Móstoles, sin embargo, si el juicio lo tiene en los juzgados de Plaza de Castilla, difícilmente podrá llegar antes del mediodía. ***Para que los compañeros estén coordinados es necesario que estén informados y ello implica compartir información****. El hecho de que sus propios compañeros conozcan dónde van a estar no supone una falta de seguridad ni un riesgo para la integridad física de los vigilantes, en primer lugar porque ellos no van a hacer un uso ilegítimo o ilegal de esa información, en segundo lugar, porque en esos centros existe seguridad suficiente para controlar asuntos mucho más graves que atentar contra la integridad física de un vigilante de seguridad.*

IX.- Asimismo, esta parte quiere remarcar que el uso de los datos tratados en estas comunicaciones está plenamente justificado, que no se han tratado datos más allá de los necesarios para desarrollar, gestionar y coordinar las funciones propias del puesto de trabajo y la relación laboral, ni se han utilizado para otros fines distintos que para los que se comunicaron, esto es gestionar la relación laboral.

Sin embargo, no podemos decir lo mismo del denunciante, que sin ir más lejos ha utilizado el e-mail del coordinador Don B.B.B. para realizar comunicaciones que nada tenían que ver con la relación laboral, absolutamente fuera de contexto, totalmente fuera de tono rozando lo irracional e indiscutiblemente con carácter intimidatorio, etc. Se adjuntan los correos remitidos por esta persona al coordinador […]

X.- En la misma línea al punto anterior, esta parte quiere subrayar que el denunciante hasta la fecha en la que fue despedido no se opuso ni hizo manifestación alguna sobre el hecho de que se utilizase su correo electrónico como canal de comunicación para organizar y coordinar el servicio, horarios,

cursos, etc. Durante el año que estuvo aproximadamente en la empresa se quejó de muchas cosas, pero en ningún momento de que no quisiese que sus compañeros de trabajo dentro del ámbito de la empresa tuviesen la dirección electrónica que facilitó él mismo, o que supiesen su número de DNI, o de las horas que tenía pendiente, o del centro asignado. Todos y cada uno de los vigilantes de seguridad tienen firmado un acuerdo de confidencialidad que recoge el compromiso de que la información relativa a la empresa permanezca restringida a ese ámbito y hasta la fecha, no se ha producido ningún incidente al respecto.

XI.- Asimismo a esta parte le parece importante pone sobre aviso al Inspector de este procedimiento, e investigue las verdaderas intenciones del denunciante, que nada tienen que ver con hacer cumplir la normativa de protección de datos, sino que su principal objetivo es castigar a una empresa por haber prescindido de sus servicios.

El espíritu de la normativa sobre protección de datos es que el interesado tenga en todo momento el control de sus datos. En este caso, los datos personales de los trabajadores se han mantenido bajo estructura de Prosegur, sin que se hayan utilizado para una finalidad distinta que para la que se obtuvieron, siempre cumpliendo la normativa y las obligaciones de informar y solicitar el consentimiento, sin que se produzca ningún incidente.

La normativa sobre protección de datos busca proteger al interesado para que no pierda el control de sus datos, para que las empresas no abusen de esa información para vender más ni se beneficien del hecho de conseguir información a cualquier precio prescindiendo absolutamente de la legalidad. La normativa sobre protección de datos vela para que se cumplan unas normas o unas formalidades con el fin de evitar que estas personas pierdan otros derechos íntimamente ligados a éste, como el derecho al honor, a la intimidad y a la propia imagen, que nada tienen que ver con el supuesto que nos ocupa.

Puede que existan cuestiones que se puedan mejorar, pero el ánimo de esta ley y del órgano al que me dirijo no es favorecer el tipo de pretensiones que tiene el denunciante."

Aportan la siguiente documentación:

copia de un correo electrónico remitido por el denunciante al coordinador el 10/04/2014 donde se presenta e indicaba que ese es su correo personal e intransferible.

copia de las cláusulas adicionales del contrato de trabajo de los vigilantes, en el que se comprometen entre otras cuestiones a no revelar los datos de carácter personal de otros trabajadores. También se recoge su consentimiento para el tratamiento de sus datos personales.

copia de los correos electrónicos remitidos por el denunciante al coordinador, y que los representantes de la entidad manifiestan ser de carácter intimidatorio.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección

de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Denuncia a la empresa **PROSEGUR** por comunicar a todos los trabajadores través de email toda la información relativa al servicio que les corresponde, figurando en destinatarios de los correos electrónicos los nombres y apellidos de todos los vigilantes de seguridad afectados, además de comunicar también a través del email los juicios a los que algunos vigilantes de seguridad han de asistir como testigos, a cuyo efecto aporta copia de correos electrónicos donde figuran los nombres y apellidos y DNI de los trabajadores así como los datos personales relativos a juicios en los que han de comparecer en calidad de testigos.

La LOPD en su artículo 3, define:

"h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

El artículo 6.1 de la LOPD, que consagra, el principio de consentimiento, dictamina:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. 2 No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento..."

La LOPD en su artículo 3 define en términos muy amplios el termino tratamiento de datos como*: "Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11 (FJ. 7 primer párrafo)… "*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)*".

Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus

datos personales y a saber de los mismos.

El tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.

III

Cuestión similar a la ahora planteada, han sido resueltas por Resoluciones de archivo por esta Agencia, entre ellas, las dimanantes de los procedimientos, E/2891/2010, E/4562/2011 sobre los medios de comunicación empleados en cuestiones laborales en el ámbito de la empresa.

De acuerdo a lo establecido por la LOPD, como hemos visto en el punto anterior, el "consentimiento" se erige como una de las piedras angulares del principio de protección de los datos de carácter personal. Así, el tratamiento de los datos del particular por parte de un tercero, en principio, sólo se puede llevar a cabo en el caso de que el titular de los mismos autorice dicho tratamiento, estableciéndose la posibilidad de que dicha autorización sea revocada en cualquier momento. Sin embargo, a lo largo de la LOPD se prevén determinados casos en los que el tratamiento de los datos de un particular no requiere del consentimiento que es exigido como regla general. Un ejemplo de dicho caso se da cuando aquél que realiza el tratamiento está ligado al titular de los mismos mediante una relación laboral, como se recoge en el citado apartado 2 del artículo 6.

En cuanto a la relación laboral, el Estatuto de los Trabajadores aprobado por el Real Decreto Legislativo 1/1995, de 24 marzo, establece en su artículo 20. 2 que: *"En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres."* Junto a ello, el artículo 20.3 E.T. dispone lo siguiente *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso."* El citado artículo, habilita al empresario a establecer procedimientos para la adopción de medidas de control empresarial, si bien con respeto de la dignidad humana.

La LOPD en su artículo 4, recoge:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Sobre el tratamiento de datos de carácter personal en el contexto profesional se ha pronunciado el Grupo de Trabajo previsto en el artículo 29, de la Directiva 95/46, que es un órgano asesor independiente que engloba a los representantes de ámbito europeo. En su Opinión 8/2001, adoptada el 13 de septiembre de 2001, prevé en el ámbito laboral el tratamiento de determinados datos por parte del empresario para el cumplimiento de sus finalidades, si bien sujeto a determinadas condiciones, al recoger:

"Que asumiendo que los trabajadores han sido informados y el proceso es legitimo, el dato personal debe ser adecuado, relevante y no excesivo en relación con las finalidades para las cuales han sido recogidos y para las finalidades para las cuales han sido tratados posteriormente.

Asumiendo que los trabajadores han sido informados de la operación de tratamiento y presumiendo que el tratamiento es legítimo y proporcional, el tratamiento debe siempre ser justo con el trabajador

Esta exigencia de responsabilidad potencialmente extensa presenta varios aspectos en el contexto profesional. En todo momento, el más importante de estos efectos es que el empleador deberá siempre tratar los datos de carácter personal de la manera menos intrusiva posible.

Varios elementos son a tomar en cuenta para asegurar la discreción: los riesgos en curso, la clase de datos implicados, la finalidad del tratamiento".

En base a lo expuesto, el Grupo del artículo 29 incluye en el citado documento un ejemplo según el cual los empleadores tal vez pueden tener necesidad de conocer para ciertos empleos si los candidatos poseen un coche y si tienen el permiso de conducir y derecho de pedir esta información, pero sería contrario a este principio el exigir el modelo o el color del coche en cuestión. En definitiva, la naturaleza de un puesto de trabajo puede requerir el uso de determinados datos que no quedaría justificado en otro puesto.

Junto a ello la Guía de Protección de Datos en las Relaciones Laborales accesible a través de www.agpd.es resulta clarificadora respecto a posibles modificaciones en el tratamiento de datos durante el desarrollo de la prestación laboral y a la necesidad de informar al trabajador:

"Las relaciones laborales son dinámicas y pueden estar sujetas a cambios sobrevenidos tanto desde el punto de vista del trabajador como desde la perspectiva de la empresa.

Por ello será necesario informar al trabajador en todos aquellos casos en los que se produzcan cambios que afecten al tratamiento de los datos personales como la aparición de nuevas finalidades o de nuevos tratamientos"

IV

A fin de valorar la justificación de la denuncia contra PROSEGUR se llevó a cabo una inspección consistente en recabar la documentación relativa a la justificación de los hechos denunciados, se confirma, entre otras aseveraciones, el hecho indubitado con

un correo del denunciante a dicha compañía que fue él quien facilitó su dirección de correo electrónico a su coordinador y que con anterioridad se le había informado acerca del uso que se le iba a dar prestando su consentimiento para ello. Es más, durante toda su relación laboral que comienza en el mes de abril de 2014 hasta el mes de mayo de 2015 se utilizó su cuenta de correo particular para remitir todas y cada de las comunicaciones, que recibe con copia a otros de sus compañeros, sin que en ningún momento manifestase su disconformidad u oposición en tanto duró la relación laboral, conducta que patentiza la prestación de su consentimiento para el tratamiento de su dirección de correo para el mantenimiento de la relación laboral.

Expuesta la inconsistencia de la denuncia, se estima aclarativo hacer una breve referencia a las contestaciones de PROSEGUR a las diferentes cuestiones planteadas por la inspección:

a) Respecto al origen de las direcciones de correo electrónico particulares que se utilizan para la remisión de correos con fines laborales por PROSEGUR, indica que fueron facilitadas por los propios empleados como lo acredita el correo electrónico remitido por el denunciante al coordinador del servicio consintiendo su tratamiento. Dicha compañía argumenta que dada la singularidad de la prestación de servicios en empresas externas no dota a los vigilantes de dirección corporativa.

b) En relación al motivo por el que no se remiten los correos electrónicos con copia oculta, alegan que por razones organizativas internas resulta imprescindible que todas las personas afectadas por un servicio se conozcan entre ellas y que los trabajadores afectos a un mismo servicio sean informados conjuntamente del cuadrante, de un cambio de turno, de una baja de un compañero, de un curso al que tienen que asistir, de forma que puedan coordinarse entre ellos y redunda en su beneficio. Reitera que las direcciones de correo electrónico se han utilizado siempre con el consentimiento de los trabajadores afectados, que son ellos los que la facilitan de "motu proprio" y se utiliza para la finalidad para que se recabaron: gestionar el servicio.

c) Respecto a la acreditación documental del consentimiento otorgado por los trabajadores para el tratamiento de sus direcciones de correo personales, así como para su comunicación al resto de trabajadores, adjuntan copia de las condiciones adicionales que firman los vigilantes de seguridad junto con el trabajo de contrato dónde se autoriza a Prosegur a tratar los datos de carácter personal de sus trabajadores que faciliten a lo largo de la relación laboral.

d) En lo concerniente a las razones para informar sobre las horas de absentismo o a recuperar de unos trabajadores a otros, esta información la facilita el coordinador a los miembros del mismo equipo o centro, en su beneficio, para que puedan coordinarse entre ellos. El conocimiento de esas horas y su necesidad de recuperación permite que el grupo de personas asignado a un servicio a que conozca la razón por la que uno de los miembros del equipo asignado realiza o no más horas en un cuadrante.

e) Sobre el hecho de que en la hoja de firmas para acreditar la asistencia a un curso aparezcan el nombre y apellidos de cada trabajador que va a asistir al mismo junto con su número de DNI. es un dato cuya utilización es necesaria dentro del ámbito de la empresa para identificar a los trabajadores que van a participar en el curso, u otra finalidad referente al mismo, no constando que se haya utilizado fuera del ámbito de la empresa por lo que supone un tratamiento justificado.

f) Finalmente, respecto a la justificación del tratamiento del centro de trabajo o servicio al que van a estar asignados cada uno de los trabajadores se lleva a cabo por temas de organización y coordinación, si bien la información recogida en el e-mail no refleja el domicilio de ninguno de los trabajadores.

Asimismo, señalan que es necesario que los compañeros conozcan la fecha y hora a las que los compañeros están citados a los Juzgados y que no van a poder asistir al trabajo, sin que conste que se haya hecho uso ilegal de dicha información.

Habida cuenta lo expuesto, dado que en el caso analizado se cuenta con el "consentimiento" del denunciante y que los tratamientos denunciados se consideran proporcionales para el fin pretendido, esto es, el desarrollo y mantenimiento de la relación laboral y que se encuentran circunscritos al ámbito interno de la empresa, procede el archivo de las Actuaciones.

No obstante se considera **NECESARIO** que se utilicen el menor número posible para la finalidad de comunicarse entre la empresa y los vigilantes jurados.

Y que el T.S en Sentencia de 21/09/2015, tiene declarado que son abusivas las cláusulas de los contratos laborales que llevan al trabajador a entregar a la empresa su número de teléfono móvil y su dirección de correo electrónico.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a ***PROSEGUR ESPAÑA SL*** y a ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, 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 del referido texto legal.

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