Expediente Nº: E/07034/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante PROSEGUR SERVICIOS DE EFECTIVO DE ESPAÑA SL en virtud de denuncia presentada por DOS DENUNCIANTES, teniendo como base los siguientes

HECHOS

PRIMERO: Las presentes actuaciones se originan por la estimación el 19/12/2017, del recurso de reposición RR/00831/2017 contra la resolución del PS/00212/2017 de 9/10/2017, que queda anulada por no haberse tenido en cuenta las alegaciones al acuerdo de inicio de la denunciada PROSEGUR SERVICIOS DE EFECTIVO DE ESPAÑA SL, pasando directamente a la resolución, sin realizar propuesta de resolución. El recurso abre nuevas actuaciones previas E/07034/2017.

SEGUNDO: Con fecha 25/01/2018 se incorporan las actuaciones previas E/3691/2016, y del subsiguiente PS/0212/2017, hasta su resolución de 9/10/2017 junto con el posterior recurso de reposición RR/831/2017, de 19/12/2017. En concreto forman parte de las mismas:

2.1 Se parte de los hechos de que el 2/06/2016, se recibe en la Agencia Española de Protección de Datos una denuncia de denunciante 1 (en ANEXO GENERAL para denunciada y en ANEXO 1 para DENUNCIANTE 1) que dice actuar como Presidente del Comité de Centro de PROSEGUR SERVICIOS DE EFECTIVO DE ESPAÑA SL, (entidad denunciada).

En su denuncia manifiesta:

1) PROSEGUR SERVICIOS DE EFECTIVO DE ESPAÑA SL, proporciona para identificar a los trabajadores ante sus clientes unas tarjetas en las que se hace constar además de nombre y apellidos, el número del documento nacional de identidad (DNI).

Aporta copia de un escrito dirigido a la empresa el 5/05/2016 solicitando que "*quitara de los listados que proporciona a sus clientes el DNI de los trabajadores, así como, que proporcionara nuevas tarjetas de identificación en las que no apareciera el DNI*", "*tarjetas de identificación internas con las cuales*" "*estamos obligados a identificarnos ante un cliente, donde no conste el número de DN*I" y que "*en los listados que se proporciona a los clientes no conste ni el DNI ni ningún otro dato que vulnere la LOPD*".

Aporta copia de la tarjeta en la que se ve en el centro el logo de la empresa, en la parte izquierda un número con tres letras, debajo el nombre y apellidos, debajo de este sin indicar que sea el número del DNI, los números de este y la letra del NIF, y en la parte derecha una fotografía.

Alude el denunciante para su pretensión, por comparación, a la sentencia del Tribunal Supremo, recurso de casación 49/2014 que trata de la impugnación de la Orden del Ministerio del Interior INT 318/2011 sobre personal de seguridad privada, que trata el asunto del número de tarjeta de identidad profesional del personal (TIP) de seguridad privada, concordancia con el número del DNI: exhibición frente a terceros de un dato de carácter personal: vulneración del deber de secreto. La sentencia indica no haber lugar al mismo y confirmar la de la Audiencia Nacional, de 20/11/2013, sala de lo contencioso, sección quinta, recurso número 201/2011.

El denunciante aporta el 20/07/2016, en segunda instancia, a requerimiento de la AEPD:

Escrito de PROSEGUR dirigido al denunciante (en representación del *Comité del Centro de Trabajo*), de 31/05/2016, mediante el que dan respuesta a "*Solicitud exclusión DNI en tarjetas de empleado y listado de clientes"*, informando de:

"Respecto a las tarjetas internas de identificación de los empleados, éstas se utilizan para identificar a los mismos, y dado que pueden existir trabajadores cuyo nombre y apellidos coincidan, resulta proporcionado incluir el dato relativo al DNI. En este sentido, se ha pronunciado repetidamente la Agencia Española de Protección de Datos (AEPD) en sus informes jurídicos, entre otros, los números 28/2011 y 666/2008."

"Por otro lado, la AEPD se ha pronunciado en los informes jurídicos 380/2009 y 413/2008, en aplicación de la normativa de prevención de riesgos laborales, indicando que resulta proporcionado que el empresario principal solicite una relación de los trabajadores que acuden a su centro de trabajo, junto con su DNI, para poder confirmar su identidad y así evitar usurpaciones.

La sentencia a la que hacen referencia en su escrito se refiere a la Tarjeta de Identificación Profesional de Vigilante de Seguridad, no a las tarjetas internas de identificación de empleados".

Relación de lugares de trabajo donde prestan servicios, que comprende casinos, estación de autobuses, establecimientos comerciales, entidades financieras, Banco de España.

2.2: En fase de actuaciones previas, E/3691/2016, los Servicios de Inspección de la AEPD solicitaron información a PROSEGUR SERVICIOS DE EFECTIVO ESPAÑA, S.L., que el 16/02/2017 indica:

PROSEGUR es una empresa de seguridad privada habilitada por el Ministerio del Interior para, entre otras, prestar las actividades descritas en el artículo 5.1 de la Ley 5/2014, de 4/4, de Seguridad Privada.

Con respecto a la TIP, su emisión corresponde al Ministerio del Interior, que la entrega directamente al titular, y se regula por el artículo 27 de la Ley 5/2014 en el que se establece que dicha tarjeta "*constituirá el documento público de acreditación del personal de seguridad privada mientras se encuentra en el ejercicio de sus funciones profesionales".*

Por otra parte la Orden INT/318/2011, de 1/02, sobre personal de seguridad privada en el artículo 14:"t*arjeta de identidad profesional"* establece que dicha tarjeta tendrá las características que se determinan en el anexo V de la presente Orden

Anexo V: *Características de la tarjeta de identidad profesional:* en el que se define el tamaño, formato y contenido y, en concreto, en el reverso lo siguiente:

Nº de tarjeta de identidad profesional: que coincidirá con el número de Documento Nacional de Identidad o del número de Identificación de Extranjero, con todos sus caracteres alfanuméricos.

Apellidos y nombre (…).

Así, la Tarjeta de Identificación Profesional de Vigilante de Seguridad (TIP) es un documento público, cuyas funciones, formato y contenido se definen en la normativa de seguridad privada.

Con respecto a la Tarjeta de Identificación de Empleado: es un documento de carácter privado que se emite por parte de la empresa con la finalidad de que el personal que accede a las instalaciones de PROSEGUR, a través de los tornos automatizados o controles de seguridad físicos, puedan identificarse debidamente.

Conforme con la normativa de aplicación, ORDEN INT/314/2011, de 1/02, sobre empresas de seguridad privada, por la propia seguridad del inmueble y de las personas que se encuentran en el mismo, es necesario poder conocer en todo momento el acceso del personal, y que el personal que ejerce funciones de vigilancia, a su vez, pueda identificar al personal comprobando su DNI y su condición de empleado lo que se hace por medio de la citada tarjeta.

La tarjeta aportada por el denunciante con el escrito de denuncia ante la Agencia corresponde con la Tarjeta de Identificación de Empleado, documento privado, de carácter interno, que se utiliza para acceder a las instalaciones de PROSEGUR.

Con respecto a la causa por la que PROSEGUR facilita a sus clientes, entidades externas, la relación de empleados que prestan servicios en las mismas con el DNI, manifiestan:

Los servicios de seguridad privada, por su propia naturaleza, se prestan en los establecimientos o inmuebles de los que es titular el cliente de PROSEGUR.

Con carácter general, en cumplimiento de la normativa de Prevención de Riesgos Laborales, Real Decreto 171/2004, de 30/01, por el que se desarrolla el artículo 24 de la Ley 31/1995, en materia de coordinación de actividades empresariales, mediante la que se impone al empresario principal un deber de control sobre los trabajadores de otras empresas que coinciden en su centro de trabajo. Para realizar ese control es necesario que el titular, del centro de trabajo, trate datos personales de los trabajadores de las empresas contratadas o subcontratadas, durante la vigencia de la relación contractual, con la finalidad de evitar o disminuir los riesgos derivados del trabajo.

Con carácter especial, en cumplimiento de la normativa de Prevención de Blanqueo de Capitales, Ley 10/2010, de 28/04, de prevención del blanqueo de capitales y de la financiación del terrorismo, PROSEGUR es un sujeto obligado y es necesario que conserve datos de los intervinientes en las operaciones de recogida/entrega por cuenta de entidades financieras, así como intercambiar información con otros sujetos obligados.

2.3 Se obtiene e incorpora la impresión de la sentencia de la Audiencia Nacional de lo contencioso administrativo, de 20/11/2013 recurso 208/2011 sobre la impugnación de la Orden del Ministerio del Interior INT/318/2011 y de la citada orden imprimida en el BOE, que

figuraban en las previas E/3691/2016. Esta sentencia fue la que luego se recurrió en casación ante el Tribunal Supremo, recurso 49/2014.

2.4: Se incorpora el informe de actuaciones previas E/3691/2016 y el acuerdo de inicio del PS/00212/2017 de 24/05/2017 en el que la Directora de la AEPD acordó iniciar procedimiento sancionador a PROSEGUR SERVICIOS DE EFECTIVO ESPAÑA, S.L. por una infracción del artículo 4.1 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

2.5: Se incorporan del citado PS/212/2017:

1) Alegaciones que la denunciada presentó el 7/07/2017 al acuerdo de inicio. En las mismas manifestaba:

-Realiza actividad de custodia, recuento, depósito de joyas, metales, billetes, obras de arte según lo detalla el artículo 5 de la Ley de Seguridad privada, así como su transporte y distribución y en los lugares en los que se lleva a cabo dichas actividades, según el artículo 7 de la Ley de Seguridad privada, han de figurar equipos o sistemas de captación de imágenes con capacidad para identificar a autores, sean delitos contras las personas o contra la propiedad, para el control de acceso de personas y vehículos, zonas de carga y descarga. También la entidad ha sido designada operador crítico por parte del Centro Nacional de Infraestructuras críticas en el que figuran además de una normativa y medidas aplicables que implican la identificación

-Falta de motivación del inicio del procedimiento sancionador sin precisar porque es excesivo o no adecuado el hecho de dar a conocer el DNI al cliente, entendiendo que las especiales medidas de seguridad conllevan el tratamiento del DNI.

-Existen informes jurídicos de la AEPD como el 28/2011 que reconoce la proporcionalidad de la inclusión del dato DNI en tarjetas de empleado en el interior de cualquier edificio de oficinas, que el tratamiento deriva de la relación contractual y no precisa el consentimiento del afectado pues sirve para identificar y garantizar la identificabilidad en el desempeño de sus funciones siendo adecuada y no excesiva

-La Sentencia de la AN que consideraba que el DNI no había de figurar en la TIP se basa en que no existe amparo normativo para ello, pero también en el exceso del dato porque el DNI sería visto por el ciudadano previsto no por la exhibición cuando se identificara.

2) Copia de la Sentencia del Tribunal Supremo sentencia 905/2016, recurso de casación 49/2014 contra la sentencia de 20/11/2013 de la sección quinta de la sala de lo contencioso administrativo de la Audiencia Nacional.

3) La respuesta de 10/01/2011 del Gabinete Jurídico de la AEPD a las consultas planteadas por la Agrupación Sindical Profesional personal habilitado de seguridad privada, sobre modo de identificación de los profesionales de seguridad privada en los juicios, a través como ejemplo de la exposición en la entrada de la sala de vistas de los Juzgados de un listado con juicios a celebrar en los que se identifican los datos personales de los vigilantes de seguridad. El informe analiza la exposición pública de los datos de los vigilantes y que en este caso aunque no deliberadamente, si se produce una puesta en conocimiento de terceros de los datos constitutiva de infracción del deber de secreto, aunque pretende contribuir a la información pública y que puede ser corregida de modo que se cohoneste la información de la actuación procesal con la protección de datos, en concreto referido a la citación a los vigilantes de seguridad. Examina el principio de calidad de datos en relación con el papel de los vigilantes de seguridad en los procesos judiciales en los que suelen ser

testigos de actos presuntamente delictivos, aconsejando la sustitución de datos identificativos con un número de identificación a semejanza de los miembros de los cuerpos de Fuerzas de Seguridad del Estado.

El segundo punto de la consulta contestada se refiere a la intención del Ministerio de Interior de usar el número del DNI como número de identificación ante los ciudadanos y que figurara en la TIP y en la placa.

La AEPD precisa que en relación con los vigilantes de seguridad, no existe una norma que autorice la exhibición a los ciudadanos de un indicativo que contenga en forma visible el DNI de un vigilante de seguridad y que se produce una infracción del deber de secreto si se adoptaran dichas decisiones, añadiendo que además, se han de atender los principios de que cuando el tratamiento de datos sea legal, debe limitarse a lo que sea necesario y suficiente al fin que se persiga.

4) Resolución de 9/10/2017 de la AEPD referencia R/02659/2017 en la que se impone una sanción a la denunciada por una infracción del artículo 4.1 de la LOPD, y se indica que no realizó alegaciones al acuerdo de inicio.

5) Escrito de recurso contra la mencionada resolución, de 2/11/2017. En el mismo se indicaba que si se habían presentado alegaciones al acuerdo de inicio, por lo que se tenía que haber emitido propuesta de resolución con audiencia. También reitera alegaciones ya producidas en el acuerdo de inicio. Añade que no todo el personal que está contratado por una empresa de seguridad tiene la condición de vigilante de seguridad y ostenta una TIP de vigilante de seguridad.

6) Resolución del escrito como recurso de reposición, estimando la anulación del PS/212/2017 y abriendo nuevas actuaciones previas E/7034/2017 para resolver la denuncia.

TERCERO: Ya en las actuaciones previas E/7034/2017, se solicitó el 31/01/2018 a la denunciada:

1) Sobre la constancia del datos DNI en las tarjetas internas de la Compañía de los vigilantes de seguridad, se le pregunta si se informa a los empleados de la recogida del DNI para tratarlo en la tarjeta interna antes de confeccionarla, o cuando se entrega o entregó a los empleados en cuanto a sus usos y deberes y obligaciones, en qué términos y que formato se hace, (copia si es escrito) desde cuando se viene usando el dato en la tarjeta, y si continua.

Con fecha 14/02/2018 reitera que se emite con la finalidad de que este personal que accede a las instalaciones de PROSEGUR, a través de los tornos automatizados o controles de seguridad físicos, pueda identificarse debidamente. Indica que la Orden INT/314/2011, de 1/02, en su artículo 7 establece para las empresas que se dedican a depósitos de fondos o valores que tienen que tener un sistema de control de accesos de personas y vehículos. Por la propia seguridad del inmueble y de las personas que se encuentran en el mismo, es necesario poder conocer en todo momento el acceso por parte del personal a dichas instalaciones y que el personal que ejerce funciones de vigilancia, a su vez, pueda identificar debidamente, una vez se ha accedido a dichas instalaciones, al personal comprobando su nombre, D.N.I. y su condición de empleado (lo que se hace por medio de la citada tarjeta).

La tarjeta se entrega en el momento en que la persona suscribe el contrato de trabajo y forma parte del personal. El uso de la tarjeta viene haciéndose desde el momento en que PROSEGUR SERVICIOS DE EFECTIVO ESPAÑA, S.L. comenzó a operar como empresa de seguridad, julio del año 2013.

La tarjeta continua usándose si bien desde el requerimiento de información E/03691/2016 y la incoación del procedimiento sancionador PS/00212/2017, de las nuevas tarjetas se ha suprimido el dato del D.N.I. y de las antiguas se están sustituyendo progresivamente.

2) Si se considera que forma parte del contrato, información que en este se da sobre dicho dato DNI en relación con uso y fines de la tarjeta interna de la compañía.

Manifiesta que se considera parte del contrato aunque no se contempla de manera expresa en el mismo, es sólo un método de acceso a las instalaciones.

3) Respuestas que se dan o han dado a las personas que ejercen el derecho a oposición al tratamiento del DNI en dichas tarjetas por considerarlo no ligado de modo inherente a la necesidad para la prestación del servicio.

Manifiesta que "*No nos consta el ejercicio del derecho de oposición al tratamiento del DNI en las tarjetas internas de la Compañía*."

4) Informe si cada empleado que presta servicios en terceras empresas lo hacen en la misma permanentemente o además si hay servicios que los desempeñan empleados indistintos habitualmente.

Manifiesta que habitualmente los servicios son desempeñados por diferentes empleados y lo hacen indistintamente. No obstante, también existen servicios que por sus especiales características suelen ser realizados con la mínima rotación posible de personal (permisos especiales, habilitaciones, accesos a infraestructuras críticas, etc.).

5) Copia de algún listado en los que usualmente ponen en conocimiento de las empresas a las que prestan servicios los datos de empleados que van a prestar servicios en las mismas y en los que se contiene el DNI. Añadir si prestan servicios permanentemente en dichos centros o puede no ser así, y si han de presentar la tarjeta interna cuando acceden a dicha tercera empresa. Si la entrega de dichos datos y listados se efectúa en desarrollo de algún convenio o contrato en la prestación de servicios, aporten copia del mismo.

Se acompaña como documento núm. 1 copia ejemplo de los listados que se envían a las empresas a las que prestan servicios al objeto de que puedan proceder a la preceptiva identificación de las personas autorizadas a entregar y retirar fondos. Se trata de un listado de personal autorizado a retirar fondos en la sede Banco de España, Murcia, figurando apellidos y nombre, código de empleado y DNI completo, con sello a 18/01/2018.

"*Como se ha indicado, los servicios son desempeñados por diferentes empleados y lo hacen indistintamente. No obstante, también existen servicios que por sus especiales características suelen ser realizados con la mínima rotación posible de personal (permisos*

especiales, habilitaciones, accesos a infraestructuras críticas, etc.). El personal de esta empresa no debe mostrar la tarjeta interna cuando acceden a dicha tercera empresa ya que su uso sólo es válido en las instalaciones de la compañía.

La prestación del servicio a nuestros clientes parte de la relación jurídica establecida en el contrato de prestación de servicios que se formaliza con los mismos pero la entrega de datos y listados se efectúa en cumplimiento de normas y políticas internas de nuestros clientes. Por ejemplo y siguiendo el hilo del listado ejemplo del documento núm. 1, para el servicio que se presta al Banco de España, la entrega de datos se efectúa en cumplimiento de la *Aplicación Técnica de Efectivo 1/2016 de servicio de caja ordinario del Banco de España para billetes y monedas en euros*, de la que aportan copia en documento núm. 2, disponible en la web del Banco de España. Esta disposición desarrolla las cláusulas generales aplicables al servicio de caja ordinario del Banco de España para los billetes y monedas en euros aprobadas por la Comisión Ejecutiva del Banco de España el 27/10/2006 y modificadas el 22/05/2015, cuya versión consolidada ha sido publicada en el Boletín Oficial del Estado del 26/05/2015. Según lo dispuesto en la *cláusula XVIII, Modificación y desarrollo,* el Banco de España puede dictar los actos necesarios para el cumplimiento del contenido de las Cláusulas Generales.

El punto 2.1 indica: "*Las entidades adheridas podrán realizar operaciones de ingresos o disposiciones (retiradas) de billetes y/o monedas en todas las sucursales del Banco de España con servicio de caja a entidades de crédito, en las dependencias del Banco de España en Madrid y, en su caso, en los centros operativos del Sistema de Depósitos Auxiliares (en lo sucesivo, SDA) a los que se encuentren adheridas*" "*Las operaciones se realizarán previa identificación de, como mínimo: a) la entidad ordenante; b) el importe total de la operación que se ha de realizar; c) el detalle por denominaciones de los billetes y/o monedas que se solicita entregar o recibir; d) el punto de distribución en el que se realizará la operación, y e) en su caso, la compañía de transporte de fondos que realiza el ingreso o disposición en su nombre*.

Se trata de las operaciones realizadas por Compañías de transporte de fondos CTF y en su punto 2.8 se contempla que para poder realizar operaciones de ingreso en efectivo o disposiciones, la CTF debe remitir al Banco de España unas listas suscritas por persona con poder bastante con la identificación de las personas físicas, empleadas de dichas compañías, autorizadas a realizar las operaciones antes referidas, estas personas deberán presentarse en las dependencias del Banco de España para la recogida de su firma previa identificación. Para que la CTF lleve a cabo operaciones de ingreso en efectivo o disposiciones, "*debe aportar la lista de personas autorizadas referidas.*"

C) Con fecha 20/02/2018 tuvo entrada un escrito del representante del Comité de Centro de PROSEGUR SERVICIOS DE EFECTIVO ESPAÑA SL, DENUNCIANTE 2 en que, aludiendo al PS/212/2017 indica que desde el acuerdo de inicio se ha empezado a retirar el DNI de las tarjetas de uso interno en la empresa, "*empezando desde este momento a identificarnos en el desempeño de nuestra función con la tarjeta de identidad profesional habilitada por el Ministerio del Interior*". Manifiesta que "*el pasado 3/01/2018 la empresa me hace llegar un documento en el cual obliga a los vigilantes de seguridad de Prosegur Servicios Efectivo España SL a identificarse ante la Seguridad Privada del Banco de España con el DNI y el TIP*", adjunta copia del documento declarando que se está incumpliendo la legalidad en

protección de datos. En el documento titulado "*Protocolo de identificación del Banco de España*" firmado por el Departamento de Operaciones a 31/01/2018, se indica:

"*El protocolo de seguridad del Banco de España nos exige para poder autorizar el acceso a sus instalaciones es necesario presentar el DNI, pasaporte o NIE como únicos documentos válidos para la identificación personal y el TIP como documento que por normativa acredita tener las habilitaciones para poder realizar las tareas de recogida y entrega de efectivo" "Por lo anterior, les recomendamos que en caso de que, por parte de personal autorizado , vigilantes de seguridad y/o Fuerzas y Cuerpos de Seguridad se les solicitara dicha documentación es preceptiva su presentación, al tratarse de un protocolo del cliente de obligado cumplimiento*".

Se le contesta que dicho documento se incorpora a las presentes actuaciones y se le informa de la finalización del PS/212/2017.

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 13712, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Se definen en el artículo 3 de la LOPD:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables; y en la letra c define: "Tratamiento de datos": "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."

c) Tratamiento de datos: 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.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

III

Señala el artículo 6 de la LOPD:

"*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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6 , de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado."

En principio, el número del DNI del empleado es necesario para el desarrollo de la relación contractual con el empleador, que lo suele utilizar para diversos fines, envío de datos a Agencia Tributaria, cotizaciones a Seguridad Social, etc. Para ello no se necesita el consentimiento del empleado.

En cuanto a su envío a terceras empresas, clientes de PROSEGUR del dato DNI con finalidades expuestas de verificación del empleado, se debe añadir que en el desarrollo reglamentario del artículo 6.2 de la LOPD, debe tenerse en cuenta que el artículo 10.2.b) del RD 1720/2007, de 21/12, de desarrollo de la LOPD, fue objeto de anulación por la STS 8/01/2012, recurso 25/2008, por exigir para aplicar la excepción a la regla general del consentimiento y así legitimar el tratamiento o cesión de los datos que estos figurasen en " *fuentes accesibles al público*".

Autorizaba el precepto reglamentario, al igual que el legal que desarrollaba, el tratamiento o cesión de datos de carácter personal sin necesidad de consentimiento del afectado cuando los datos figurasen en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tuviera un interés legítimo para su tratamiento o conocimiento, siempre que no se vulnerasen los derechos y libertades fundamentales del interesado.

La razón de esta anulación y, por ende, la interpretación que ha de hacerse del tanto del artículo 6.2 de la LOPD se encuentra en el texto del artículo 7 de la mencionada Directiva 95/46, de 24/10, donde se establece lo siguiente:

"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no

prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva: en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales."

Además, la interpretación que ha de hacerse del artículo 6.2 de la LOPD en relación con el artículo 7 de la mencionada Directiva 95/46, de 24/10 , se manifiesta en la respuesta a la cuestión prejudicial planteada por el Tribunal Supremo al Tribunal de Justicia de la Unión Europea, en los recursos planteados frente a determinados preceptos del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12 (en adelante RLOPD); se cuestionó la adecuación o no al derecho comunitario del mencionado artículo 10.2.b) del citado Reglamento, y que dio lugar a la sentencia antes citada..

En respuesta a tal cuestión la sentencia del Tribunal de Justicia de la Unión Europea de 24/11/2011 (Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (asunto C-468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) C-469/10) contiene los siguientes pronunciamientos:

"1. Se opone al artículo 7.f) de la Directiva 95/46 *la normativa nacional que, para permitir el tratamiento de datos, sin consentimiento, y necesario para la satisfacción de un interés legítimo (del responsable o del cesionario) exige que se respeten los derechos y libertades del interesado, y además que dichos datos figuren en fuentes accesibles al público, excluyendo de forma categórica y generalizada todo tratamiento que no figure en dichas fuentes.*

2. El artículo 7.f) de la Directiva 95/46 *tiene efecto directo"* .

Estos pronunciamientos se sustentan en la consideración de que el artículo 7, letra f), de la Directiva 95/46 establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado (apartado 38). De modo que este segundo requisito exige una ponderación de los derechos e intereses en conflicto que dependerá de las circunstancias concretas, teniendo en cuenta los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, en la cual podrán considerarse, entre otras circunstancias, que los datos figuren ya, o no, en fuentes accesibles al público.

La relevancia de tal decisión prejudicial radica en que, tal y como afirma la propia sentencia del TJUE, el objetivo de la Directiva 95/46 consiste en asegurar un nivel de protección equivalente en todos los Estados miembros, por lo que el artículo 7 de la Directiva 95/46 establece una lista exhaustiva y taxativa de los casos en que un tratamiento de datos personales puede considerarse lícito (apartado 30). De ello se desprende que los Estados miembros no puedan ni añadir al artículo 7 de la Directiva 95/46 nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo (apartado 32).

La conclusión es que, en lo que respecta al tratamiento de datos personales, el artículo 7, letra f), de la Directiva 95/46 se opone a toda normativa nacional que, en el caso de que no exista consentimiento del interesado, imponga exigencias adicionales que se sumen a los dos requisitos acumulativos mencionados en el apartado anterior (apartado 39).

Precisamente por ello, el Tribunal Supremo en su sentencia de 8 de febrero de 2012, Rec. 25/2008 , aplicando los pronunciamientos contenidos en la sentencia del TJUE, afirma

que *"Lo que expresa el Tribunal es que con la exigencia de que los datos figuren en fuentes accesibles al público se excluye de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes, y declara tal proceder contrario al artículo 7 f) de la Directiva", por lo que la circunstancia de que los datos figuren en fuentes accesibles al público, referenciada en el artículo 10.2 b) del Reglamento, no actúa como elemento de ponderación. Ninguna dificultad de redacción habría para darle ese carácter. Actúa, y a ello se refiere la sentencia en su fundamento 47, como requisito habilitante que, por adicionarse a la previsión del* artículo 7 f) de la Directiva, debe declararse nulo...". Y en consecuencia anuló el art. 10.2.b) del Real Decreto 1720/2007 de 21 de diciembre.

Idéntica conclusión ha de alcanzarse respecto a esta misma exigencia -"*cuando los datos figuren en fuentes accesibles al público*"-, contenida en el artículo en el art. 6.2 de la LOPD , por lo que tal previsión deber resultar inaplicada y tenerse por no puesta, en cuanto resulta contraria al derecho comunitario, en aplicación del principio de primacía del Derecho comunitario europeo (en igual sentido SSAN de 11/04/2012 (RJCA 2012, 338) , Rec. 410/2010 y de 15/03/2012 (PROV 2012, 187075) , Rec. 390/2010).

Por consiguiente, la interpretación correcta tanto el artículo 6 de la LOPD como el artículo 7, letra f), de la Directiva 95/46/CE , reside en la exigencia de dos requisitos acumulativos para que un tratamiento o cesión de datos personales sea lícito sin contar con el consentimiento del afectado, a saber: por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos; y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado.

III

En la denuncia no se plantea la constancia y uso del número del DNI en cuanto dato personal en una tarjeta interna que se pueda usar habitualmente por el personal, vigilante de seguridad para el acceso a las propias instalaciones. Este aspecto ha sido analizado por esta Agencia Española de Protección de Datos, emitiéndose informe de fecha 12/05/2006. En el citado informe, y en lo que respecta al dato del documento nacional de identidad, se indicaba lo siguiente:

"Con carácter general el artículo 4.1 de la Ley Orgánica 15/1999, que consagra el denominado principio de proporcionalidad en el tratamiento, establece que "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". De ello se desprende la necesidad de que el tratamiento de un determinado dato de carácter personal, (como sería, en este caso, los datos de los trabajadores afectados, toda vez que para su inclusión en la tarjeta de identificación será necesaria la realización de una o varias de las actividades definidas como de tratamiento de datos por el artículo 3 c) de la mencionada Ley), deberá ser proporcionado a la finalidad que lo motiva.

De este modo, si dicha finalidad pudiera ser suplida por la realización de una actividad distinta al citado tratamiento, sin que dicha finalidad sea alterada o perjudicada, debería optarse por esa última actividad, dado que el tratamiento de los datos de carácter personal supone, tal y como consagra nuestro Tribunal Constitucional, en Sentencia 292/2000, de 30 de noviembre, una limitación del derecho de la persona a disponer de la información referida a la misma.

En el caso sometido a la presente consulta, si la finalidad que motiva el tratamiento es la identificación del trabajador como tal, y existiendo en muchas ocasiones un número indeterminado de personas con idénticos nombres y apellidos, a nuestro juicio, no resultaría contrario a la normativa sobre protección de datos de carácter personal, la inclusión del dato correspondiente al número del D.N.I. de la persona a cuyo nombre se expide la mencionada tarjeta identificativa. En consecuencia, se considera que la inclusión, en el presente caso, del dato de D.N.I. en las tarjetas identificativas del personal no vulnera el anteriormente señalado principio de proporcionalidad, al no resultar dicho tratamiento excesivo para la finalidad de identificación del personal."

Igual argumentación cabe aplicarse al presente supuesto en cuanto a la inclusión en las tarjetas identificativas, del nº de D.N.I. y nombre y apellidos del trabajador, no pudiendo la misma considerarse excesiva a los efectos previstos en el artículo 4.1 de la Ley Orgánica 15/1999.

En el caso sometido a la presente consulta, si la finalidad que motiva el tratamiento es la identificación del trabajador como tal, para que las personas que sean atendidas por los mismos puedan referenciar la atención recibida a una persona en concreto, sería acorde con el citado artículo 4.1 de la Ley.

Por otra parte, en cuanto a la legitimación para el tratamiento de los datos en el marco del desempeño de una relación laboral o estatutaria, el artículo 6.2 de la Ley Orgánica 15/1999 dispone que "*No será preciso el consentimiento cuando los datos de carácter personal (…) 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*."

Lo que se discute y valora ahora es si la tarjeta interna de la entidad que porta dicho número de DNI, o el DNI mismo, podrían ser presentados a clientes con los que la empleadora denunciada, Prosegur tiene contratados sus servicios, y si dichos clientes pueden disponer del número del DNI anotado previamente al recibirlo de PROSEGUR, para validar que la persona que les va a prestar un determinado servicio es la que se les presenta.

En primer lugar, una norma interna del Banco de España, exige para la retirada o ingreso de billetes y monedas de efectivo esa entrega previa de dato del DNI y nombre y apellidos del empleado, figurando así en un formulario en papel que consta en la circular-instrucción del banco de España referida.

En segundo lugar, se han de tener en cuenta las especificidades de las funciones y lugares en que el personal de PROSEGUR desempeña sus funciones en terceras entidades o para terceras personas. Se puede tratar de aactividad de custodia, recuento, depósito de joyas, metales, billetes, obras de arte según lo detalla el artículo 5 de la Ley de Seguridad privada, así como su transporte y distribución. También los lugares por los que discurre dicha actividad han de contar con equipos o sistemas de captación de imágenes capaces para identificar a autores de delitos contras las personas y contra la propiedad, para el control de acceso de personas y vehículos, zonas de carga y descarga. También la entidad ha sido designada operador crítico por parte del Centro Nacional de Infraestructuras críticas en el que figuran además de una normativa y medidas aplicables que implican la identificación. Además, existen sectores en que la plena identificación de la persona es un rasgo esencial, como ejemplo, la recogida de dinero en el Banco de España o dependencias

del mismo, o de otras entidades y funciones que se han mencionado. Mostrando la tarjeta profesional y la tarjeta interna del trabajo que porta el número del DNI o el mismo DNI para dichas finalidades, encuentra acomodo en el interés legítimo por parte de PROSEGUR y el cliente, efectuando las operaciones con mayor certeza y seguridad, y por la persona señalada que pertenece a dicha entidad y ha sido designada para el servicio.

Este modo de cumplimiento de la relación jurídica que se entabla entre las partes y el interés de la operación, conllevan que dicha identificación es una práctica recomendable para la finalidad tendente a la identificación en dicho tipo de actividades, sin que se vea sacrificado el derecho del titular del dato por la mera confrontación de dicho dato que previamente se ha dado en papel, con el objeto de llevar a cabo las operaciones. Obligaciones como la mera exhibición del DNI son habituales en distintos ámbitos de la vida privada o administrativa como ejemplos, acceder a edificios o entregar una copia de un escrito a la persona para verificar que es dicha persona.

Además, esta identificación, se produce en el marco que regula el DNI, Real Decreto 1553/2005, de 23/12, que le atribuye valor suficiente para acreditar, por sí solo, la identidad de las personas, mientras que en su artículo 1.2, se precisa que "*Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen*."

Teniendo en cuenta que como regla general, los vigilantes de seguridad no son considerados autoridad pública, y que a través de la exhibición de la tarjeta de identidad profesional es el medio para identificarse ante los ciudadanos, y que en este sentido de la denuncia, no están actuando ante los ciudadanos sino ante un tercero cliente de su empresa, para las que desarrolla el servicio, no se estima desproporcionada la citada medida de comprobar a través del DNI la identidad de la persona que se asigna al servicio encomendado, dadas las características especiales en que consisten las funciones a desempeñar, como retirada de efectivo o depósito de obras de arte por nombrar solo dos específicos.

Por tanto, existiría facultad para tratar dicho dato del DNI en estas circunstancias

El artículo 126.1, apartado segundo, del RLOPD establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

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 SERVICIOS DE EFECTIVO DE ESPAÑA SL** con copia de ANEXO GENERAL, a **DENUNCIANTE 1** con copia del ANEXO 1, y a **DENUNCIANTE 2**, con copia del ANEXO 2**.**

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 30/12, 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 22/12, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21/12.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, 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