Se plantea si resulta conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, que la empresa a la que se refiere la consulta dedicada a la prestación de servicios de contact center para otras empresas, entregue una fotocopia del DNI de sus trabajadores a una entidad cliente, a fin de que dicha entidad compruebe la identidad de los trabajadores del consultante que van a acceder a sus sistemas de información.

La comunicación de los datos a que la consulta hace referencia constituye una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999, como "*toda revelación de datos realizada a una persona distinta del interesado".*

Tal cesión debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la misma Ley, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario y exige para que pueda tener lugar, el previo consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

No obstante, el número segundo del artículo 11, prevé una serie de supuestos en que se excepciona la necesidad de consentimiento del afectado por el tratamiento de datos, de las cuales interesa aquí analizar la contenida en su letra c) que podría resultar de aplicación al presente supuesto, al prever la posibilidad de cesión no consentida *"Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique."*

Para determinar si puede considerarse habilitada la comunicación de datos objeto de consulta en la excepción contenida en el artículo 11.2.c) cabe recordar, en primer lugar, lo señalado por el Tribunal Supremo, en Sentencia

de 8 de octubre de 2010, en relación a la interpretación que debe darse al dicho precepto al declarar que *"la cuestión realmente conflictiva se circunscribe a la interpretación que debe darse al artículo 11.2.c) que, conforme ya anunciamos, contiene una excepción a la regla general de la necesidad del consentimiento del interesado para la comunicación de datos a un tercero*.

Sentando como punto de partida que toda excepción a la regla general debe ser objeto de interpretación restrictiva, impidiendo extender la excepción a supuestos de dudoso encaje en la misma, es de significar el rigor con el que el legislador redacta la norma, consciente sin duda de que el principio o la regla general de la necesidad del consentimiento se erige en fundamental en un ámbito especialmente sensible, cual es el de la protección de un derecho fundamental proclamado por el artículo 18 de la Constitución y por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

Cuando el legislador utiliza en la redacción del artículo 11.2.c) el adverbio "necesariamente" en cuanto sinónimo de "inevitablemente" "irremediablemente" "indefectiblemente", etc, advierte que es forzoso, preciso, obligatorio, esencial, que la relación jurídica aceptada requiera para su desenvolvimiento la conexión del tratamiento con el fichero de terceros.

En el presente supuesto se entiende que estaríamos ante una prestación de servicios, que requiere el acceso de los empleados de la empresa que realiza el servicio, que actúa en calidad de encargado del tratamiento (artículo 12 de la Ley 15/1999), a los ficheros de la empresa cliente, siendo una de las medidas de seguridad establecida por dicho cliente en su condición de responsable de los ficheros, la comprobación de la identidad de quienes acceden a sus sistemas de información.

A este respecto, debe recordarse que el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, norma que en la actualidad contiene la regulación de las medidas de seguridad a adoptar en el tratamiento de datos personales, dispone en el número primero de su artículo 82 lo siguiente:

"1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento."

Entre tales medidas de seguridad, debe aquí hacerse referencia a la contenida en el artículo 93 de la misma norma respecto a la identificación y autenticación de los usuarios de los sistemas de información:

"1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad."

Por consiguiente, en el presente caso, debe considerarse que la cesión de datos a que se refiere la consulta, se encontraría legitimada en lo previsto en el artículo 11.2.c) de la Ley Orgánica 15/1999, al formar parte de la relación laboral de los trabajadores del consultante la prestación de servicios a un tercero, prestación que puede conllevar el acceso a los ficheros de éste, lo que comporta, en tal caso, el cumplimiento de las medidas de seguridad previstas en el documento de seguridad de dicho tercero, una de las cuales es necesariamente la identificación de forma inequívoca y personalizada de los usuarios que accedan a los sistemas del responsable del fichero.

Dicha cesión de datos deberá ser respetuosa de los principios de la protección de datos contenidos en el artículo 4 de la Ley Orgánica 15/1999, señaladamente de los principios de proporcionalidad, finalidad y conservación.

Debe así recordarse que la proporcionalidad exige, según la doctrina del Tribunal Constitucional, siguiendo a tal efecto la sentada por el Tribunal Europeo de Derechos Humanos, la superación de un triple juicio, en el sentido de determinar si la medida adoptada es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con

igual eficacia (juicio de necesidad) y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

A este respecto debe tenerse en cuenta que el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana señala respecto de la acreditación de la identidad de los ciudadanos españoles que *"Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad. El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a éstos otorgan las leyes, así como suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular."*

Por consiguiente, la entrega de la fotocopia de un documento destinado precisamente a la acreditación de la identidad de las personas debe considerarse una medida idónea, necesaria y equilibrada o ponderada para la finalidad perseguida de comprobar la identidad de las personas a quienes se va a permitir acceder a los sistemas informáticos del cliente del consultante.

Por su parte, el artículo 4.1 de La Ley Orgánica 15/1999, configura el principio de proporcionalidad en los siguientes términos "*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".*

Asimismo, el artículo 4.5 recoge el principio de conservación de los datos disponiendo que *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."

De este modo, sería conveniente que una vez entregada la fotocopia del documento de identidad con la finalidad de identificar al usuario del sistema, se destruyese la misma una vez llevada a cabo la finalidad de identificación, limitándose el cesionario a conservar los datos de identidad y DNI, lo que

vendría a dar cumplimiento a ambos principios tal y como vienen recogidos en la Ley Orgánica 15/1999.

Por último, debe recordarse que el cesionario de los datos está sujeto al principio de finalidad, consagrado en el artículo 4.2 de la Ley Orgánica 15/1999, en virtud del cual los datos "*no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*". Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión "finalidades incompatibles" como sinónimo de "finalidades distintas". De esta manera, cualquier utilización de los datos recabados para una finalidad distinta de aquella para la que se obtuvieron o una comunicación o difusión de los mismos, sin que exista causa legitimadora del nuevo tratamiento, supondría una vulneración de la citada Ley Orgánica 15/1999.