Creación de sistemas de denuncias internas en las empresas (mecanismos de "whistleblowing")

La consulta plantea la conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, del sistema interno de denuncia que se describe en la consulta, cuyas características pueden resumirse, en virtud de lo señalado en la misma, del siguiente modo:

- El sistema permitirá la denuncia de "comportamientos, acciones o hechos que puedan constituir violaciones tanto de las normas internas de la compañía como de las leyes, normativas o códigos éticos" que rigen su actividad.

- Todos los empleados de la compañía podrán ser denunciantes o denunciados en el sistema.

- Los empleados será previamente informados de la existencia y finalidad del sistema, su funcionamiento, la garantía de confidencialidad de los datos del denunciante y la garantía de información al denunciado de la existencia de la denuncia.

- El procedimiento de denuncia será telefónico o presencial.

- Sólo accederán, en principio, a los datos el responsable de "compliance counter" y las personas para las que resulte imprescindible a fin de investigar los hechos denunciados.

- El sistema incorporará los datos de denunciante y denunciado, los hechos denunciados y el resultado de las investigaciones.

- Se informará al denunciado en el plazo más breve posible de los hechos denunciados, los destinatarios de la información, el departamento responsable del sistema y sus derechos en materia de protección de datos. No se informará de la identificación del denunciante a menos que hubiera obrado con mala fe.

- Los datos serán cancelados en un plazo máximo de dos meses tras el fin de las investigaciones si los hechos no hubieran sido probados. En caso de entablarse acciones, los datos se

conservarán en tanto sea necesario para el ejercicio por la compañía de sus derechos en juicio.

- Se implantarán las medidas de seguridad de nivel básico.

- Los datos serán transmitidos a las oficinas competentes en Reino Unido y Japón, en este segundo caso se aportarán para solicitar la autorización del Director de la Agencia Española de Protección de Datos las cláusulas contractuales tipo aprobadas por la Comisión Europea.

II

Precisamente, como consecuencia de lo indicado en último lugar, es preciso efectuar una observación previa, dado que la Norma segunda de la Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos aclara que "La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento".

Ello implica que, al margen de la necesaria aportación de las garantías exigidas por el artículo 33 de la Ley Orgánica 15/1999, que se materializarían en el caso de la transferencia a Japón en la aportación de las cláusulas contractuales adoptadas por la Comisión Europea, que en este caso deberá ser las que rigen la transferencia de datos entre responsables del tratamiento, será necesario que la cesión implícita a la mencionada transferencia, así como el tratamiento de los datos en España, cumpla con lo dispuesto en la propia Ley Orgánica 15/1999.

Ello exige analizar la viabilidad del sistema a la luz de las normas contenidas en la Ley Orgánica 15/1999, con carácter previo a cualquier otra consideración, a fin de determinar si el tratamiento que implica la creación del sistema de denuncias, en los términos descritos en la consulta, puede encontrarse amparado por la Ley Orgánica 15/1999.

Como se indica en la consulta, la aplicación a las compañías europeas y a las filiales europeas de las compañías de terceros Estados de los sistemas denominados "de whistleblowing" o de denuncias ha sido una cuestión objeto de profundo y reiterado análisis por parte de las autoridades europeas de protección de datos, ya en su actuación cotidiana, ya mediante su estudio en el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, en particular en lo relacionado con la implantación de los sistemas impuesta por la Ley Sarbanes-Oxley.

Precisamente en la reunión del citado Grupo celebrada el 1 de febrero de 2006 fue adoptada, como documento WP117 la Opinión 1/2006 sobre la

aplicación de las normas de protección de Datos de la Unión Europea a los mecanismos internos de "Whistleblowing" en el ámbito de la contabilidad y los controles internos de auditoría, la lucha contra la estafa y los delitos bancarios y financieros.

Debe indicarse que dicho informe, mencionado en la consulta, se refiere únicamente a la implantación de dichos sistemas en el marco de la actuación contable y auditora, reservándose el Grupo su opinión en lo relativo a la creación de otros sistemas similares en ámbitos distintos del mencionado, como sería el planteado en el supuesto ahora analizado, referido a "comportamientos, acciones o hechos que puedan constituir violaciones tanto de las normas internas de la compañía como de las leyes, normativas o códigos éticos" que rigen la actividad de la compañía consultante, integrada en el sector farmacéutico

En el citado documento, el Grupo de Trabajo señalaba que "*Aplicar las normas de protección de datos de la Unión Europea a los programas de denuncia de irregularidades supone otorgar una consideración específica a la cuestión de la protección de la persona que pueda haber sido incriminada en una alerta. En este sentido, el Grupo de Trabajo enfatiza que los programas de denuncia de irregularidades conllevan un riesgo muy grave de estigmatización y vejación de dicha persona dentro de la organización a la que pertenece. La persona estará expuesta a tales riesgos incluso antes de saber que ha sido incriminada y de que los supuestos hechos se hayan investigado para determinar o no su fundamento"*. Asimismo, se concluía que *"El Grupo de Trabajo es de la opinión de que una correcta aplicación de las normas de protección de datos a los programas de denuncia de irregularidades contribuirá a paliar dichos riesgos. También es de la opinión de que, lejos de evitar que dichos programas funcionen de conformidad con su objetivo pretendido, la aplicación de dichas normas, por lo general, contribuirá a un funcionamiento adecuado de los programas de denuncia de irregularidades*".

III

Dicho lo anterior, debe señalarse que la implantación de los mecanismos citados y la tramitación de las quejas relacionada con los mismos se encontrará sometida a lo dispuesto en la Ley Orgánica 15/1999, al señalar el artículo 2.1, párrafo primero de la Ley que "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", siendo tratamiento, según el artículo 3 c), "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".

En cuanto a la aplicación de la Ley a los tratamientos no automatizados de datos, como podría suceder en el caso de recepción de las denuncias a partir de la personación del denunciante ante la persona responsable en la empresa, mencionada en la consulta, la doctrina de la Audiencia Nacional es plenamente uniforme en el sentido de indicar que el apartado segundo de la Disposición adicional tercera de la Ley Orgánica, que establece una demora en la aplicación de la Ley a los tratamientos no automatizados hasta el 24 de octubre de 2007, se refiere exclusivamente a los preexistentes a su entrada en vigor el 14 de enero de 2000, de modo que la Ley Orgánica será aplicable a cualquier fichero manual en el que se hubiera introducido algún dato con posterioridad a dicha fecha. Así lo señala, por ejemplo, la Sentencia de 19 de mayo de 2004.

IV

En cuanto a la habilitación o legitimación para el tratamiento de los datos, el artículo 6.1 de la Ley Orgánica 15/1999 dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. No obstante aclara el artículo 6.2 que “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 el mismo sentido, el artículo 11.1 dispone que “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”, si bien el consentimiento no será necesario “cuando la cesión está autorizada en una Ley” (artículo 11.2 a) o “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”, si bien “en este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique” (artículo 11.2 c).

Dicho esto, debe señalarse que no existe en el ordenamiento jurídico español una previsión general similar a la impuesta a "Las empresas de servicios de inversión, las entidades de crédito y las personas o entidades que actúen en el Mercado de Valores, tanto recibiendo o ejecutando órdenes como

asesorando sobre inversiones en valores" por el artículo 79.1 d) de la Ley del Mercado de Valores, consistente en "Disponer de los medios adecuados para realizar su actividad y tener establecidos los controles internos oportunos para garantizar una gestión prudente y prevenir los incumplimientos de los deberes y obligaciones que la normativa del Mercado de Valores les impone", lo que hubiera permitido fundar el tratamiento en los artículos 6.1 y 11.2 a) de la Ley Orgánica 15/1999.

De este modo, el tratamiento y cesión de los datos habrán de ampararse en alguno de los supuestos contemplados en los citados artículos 6.2 y 11.2 de la Ley Orgánica 15/1999, dado que por la propia naturaleza de estos procedimientos no se contará, obviamente, con el consentimiento de los denunciados.

Según el documento WP117, ya mencionado "*Tal y como están las cosas, dos motivos parecen ser pertinentes en el presente contexto: o bien es necesario el establecimiento de un sistema de denuncia de irregularidades para el cumplimiento con una obligación jurídica (artículo 7(c)) o a los efectos de un interés legítimo perseguido por el responsable del tratamiento o por el tercero a quien se divulgan los datos (artículo 7(f))*", ambos de la Directiva 95/46/CE.

Debe señalarse que la Agencia Española de Protección de Datos defendió en las reuniones relacionadas con la adopción de la Opinión que los motivos señalados podían no ser los únicos en los que fundamentar el tratamiento derivado de la existencia de los mecanismos de "whistleblowing". Por este motivo, el documento final omitió la expresión "solamente" que se incluía en el texto transcrito.

En particular, la Agencia consideró la posible aplicación en estos procedimientos de la legitimación conferida por el artículo 7 b) de la Directiva, que permite el tratamiento de los datos "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", objeto de transposición por los artículos 6.2 y 11.2 c) de la Ley Orgánica 15/1999, que se han reproducido en lugares anteriores de este informe.

En efecto, dado que la Ley española no impone el deber jurídico de implantar estos procedimientos y que la regla del interés legítimo ha de venir referenciada al reconocimiento del mismo por una norma legal aplicable al caso, lo que tampoco resulta claramente discernible en este caso, cabría analizar si el tratamiento al que se refiere la consulta podría encontrarse incardinado en la existencia de un vínculo contractual.

Como se indica en la consulta, los denunciantes y denunciados a los que se refiere el sistema que pretende crearse serán en todo caso empleados de la compañía, es decir, se encontrarán, en general, vinculados a la misma por una relación laboral, siendo trabajadores de la misma o, en su caso y en un sentido

amplio, mantendrán con la compañía un vínculo derivado de un contrato de arrendamiento de servicios con algún tipo de compromiso de exclusividad. En consecuencia, todas las personas cuyos datos pueden ser tratados como consecuencia del establecimiento de procedimientos de denuncia mantendrán con la sociedad un vínculo contractual de derecho laboral, civil o mercantil.

Pues bien, sería posible que siempre que existiese pleno conocimiento de la existencia de los mecanismos descritos por parte de las personas cuyos datos pudieran ser tratados por los mismos, quedando la existencia de dichos procedimientos incorporada a la relación contractual como parte integrante de la misma, el tratamiento de los datos pudiese considerarse necesario para el desarrollo y control adecuado de la relación contractual, lo que permitiría considerar el mismo amparado en la Ley Orgánica 15/1999.

No obstante, para que la conclusión anteriormente alcanzada fuera posible, sería preciso que la finalidad que justifica el establecimiento de los sistemas de denuncia descritos en la consulta resultase ajustada al adecuado mantenimiento de las relaciones contractuales, de forma que el sistema se centrase en la denuncia de conductas que pudieran efectivamente afectar al mantenimiento o desarrollo de la relación contractual que vincula al denunciado y a la consultante.

En este sentido, el artículo 4.1 de la Ley Orgánica 15/1999 consagra el denominado principio de proporcionalidad del tratamiento a la finalidad, disponiendo 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”.

Así, recuerda el documento WP117 que “*la letra f) del artículo 7 requiere que se alcance un equilibrio entre el interés legítimo exigido por el tratamiento de datos personales y los derechos fundamentales de los interesados. Este equilibrio de intereses deberá tener en cuenta la proporcionalidad, la subsidiariedad, la gravedad de los presuntos delitos que puedan denunciarse y las consecuencias para los interesados. A efectos del control del equilibrio de intereses, habrá que establecer las salvaguardias adecuadas*”.

Por todo ello, el tratamiento de datos de carácter personal derivado de la existencia del sistema de denuncia descrito en la consulta podrá resultar acorde con lo dispuesto en la Ley Orgánica 15/1999 y amparado por su artículo 6.2, en lo referente a la necesidad del tratamiento para el mantenimiento de la relación contractual, en caso de que el sistema se circunscriba a las denuncias referidas a materias o normas internas o externas cuyo incumplimiento tiene una consecuencia efectiva sobre el mantenimiento de la relación contractual entre la empresa y el denunciado, sin que sea suficiente su establecimiento en relación con cualesquiera “comportamientos, acciones o hechos que puedan

constituir violaciones tanto de las normas internas de la compañía como de las leyes, normativas o códigos éticos" aplicables a la consultante.

En consecuencia, será necesario que se aclare el contenido de dicha expresión, limitando el sistema a las denuncias relacionadas con hechos o actuaciones que tengan una efectiva implicación en la relación laboral, concretando así que acciones deberán ser objeto de denuncia y especificando las normas a las que las mismas se refieren.

Así, no puede considerarse que un sistema genérico como el descrito tiene amparo en la Ley Orgánica 15/1999 en tanto no se produzca una concreción como la mencionada, debiendo tener en consideración las actuaciones que puedan, en la práctica llevar a una situación de sanción al trabajador o empleado o a la resolución de su contrato.

V

Debe ahora hacerse referencia a los principios de exactitud y conservación, recogidos en la Ley Orgánica 15/1999.

En cuanto al primero de ellos, el artículo 4.3 de la Ley Orgánica 15/1999 dispone que "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado".

Respecto a esta materia, el documento WP117, ya citado, señala que

"Por lo que respecta a las normas de protección de datos, los informes anónimos plantean un problema específico con respecto al requisito esencial de que los datos personales sólo deberían recopilarse de manera leal. Como norma, el Grupo de Trabajo considera que sólo los informes identificados deberían comunicarse a través de programas de denuncia de irregularidades para satisfacer este requisito.

No obstante, el Grupo de Trabajo es consciente de que algunos denunciantes podrían no encontrarse siempre en situación o tener disposición psicológica para presentar informes identificados. También es consciente del hecho de que las quejas anónimas son una realidad dentro de las sociedades, incluso y especialmente en ausencia de sistemas de denuncia de irregularidades confidenciales y organizados, y que esta realidad no puede ignorarse. Por ello, el Grupo de Trabajo considera que los programas de denuncias de irregularidades podrían llevar a la presentación de informes anónimos a través del programa y a la toma de medidas basadas en ellos, pero sólo como excepción a la regla y en las siguientes condiciones.

El Grupo de Trabajo considera que los programas de denuncia de irregularidades deberían estar creados de tal manera que no fomenten

los informes anónimos como la manera habitual de presentar una queja. En concreto, las sociedades no deberían anunciar el hecho de que se permiten los informes anónimos a través del programa. Por el contrario, puesto que los programas de denuncia de irregularidades deberían garantizar que la identidad del denunciante se trata en condiciones de confidencialidad, las personas que pretendan presentar un informe mediante un sistema de denuncia de irregularidades deberían ser conscientes de que no sufrirán por su acción. Por esa razón, el programa debería informar al denunciante, en el momento de establecer el primer contacto con el programa, de que su identidad se mantendrá confidencial en todas las etapas del proceso y, en concreto, que no se divulgará a terceros, ni a la persona incriminada y a los mandos directivos del empleado. Si, a pesar de esa información, la persona que informa al programa sigue queriendo permanecer en el anonimato, el informe se aceptará en el programa. También es necesario informar a los denunciantes de que podría ser necesario divulgar su identidad a las personas pertinentes implicadas en cualquier investigación posterior o procedimiento judicial incoado como consecuencia de la investigación llevada a cabo por el programa de denuncia de irregularidades."

A nuestro juicio, debería partirse del establecimiento de procedimientos que garanticen el tratamiento confidencial de las denuncias presentadas a través de los sistemas de "whistleblowing", de forma que se evite la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas.

La garantía de la confidencialidad debería manifestarse a través del hecho de que la persona denunciada no pudiera acceder a los datos identificativos de la persona denunciante. Ello resultaría plenamente conforme a lo dispuesto en la Ley española, dado que el artículo 3 a) de la Ley Orgánica 15/1999 define los datos de carácter personal como "Cualquier información concerniente a personas físicas identificadas o identificables".

Podría plantearse que la persona denunciada podría conocer los datos identificativos de su denunciante mediante el ejercicio del derecho de acceso. Sin embargo, debe recordarse que el derecho de acceso es definido por el artículo 15.1 como el "derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos".

Pues bien, dado que el derecho queda limitado a los propios datos de carácter personal objeto de tratamiento, no puede considerarse que la información que contenga datos de terceras personas, como sucedería en este caso con los datos del denunciante, quede incluida en el mencionado derecho, toda vez que la transmisión al denunciado de dichos datos implicaría la revelación de los mismos a una persona distinta del denunciante-afectado y, en

consecuencia, una cesión o comunicación de los datos del mismo, que no encontraría amparo en los supuestos regulados por el artículo 11 de la Ley Orgánica 15/1999.

En consecuencia, el establecimiento de mecanismos que garanticen la presentación de denuncias confidenciales, y no anónimas, no perjudicaría la operatividad del sistema, al deber quedar claramente planteada la conclusión de que los datos del denunciante en modo alguno podrían ser transmitidos al denunciado con ocasión del ejercicio del derecho de acceso.

Por ello, a fin de garantizar el cumplimiento del mencionado principio deberá exigirse que el sistema únicamente acepte la inclusión de denuncias en que aparezca identificado el denunciante, sin perjuicio de las salvaguardias que se han señalado para garantizar la confidencialidad de sus datos de carácter personal, no bastando el establecimiento de un primer filtro de confidencialidad y una posible alegación última del anonimato para el funcionamiento del sistema.

VI

Por otra parte, el artículo 4.5 de la Ley Orgánica 15/1999 dispone en sus dos primero párrafos 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” y “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”.

En relación con este punto, el documento del Grupo de Trabajo señala que “*Los datos personales tratados por un programa de denuncia de irregularidades deberían eliminarse, inmediatamente, y normalmente en un plazo de dos meses desde la finalización de la investigación de los hechos alegados en el informe*”.

En este sentido, sería imprescindible que se establezca un plazo máximo para la conservación de los datos relacionados con las denuncias, a fin de evitar el mantenimiento de los mismos por un período superior que perjudique los derechos del denunciado y del propio denunciante, cuya confidencialidad debe quedar garantizada.

Este plazo debería limitarse a la tramitación de las medidas de auditoría interna que resultasen necesarias y, como máximo, a la tramitación de los procedimientos judiciales que se derivasen de la investigación realizada (como, por ejemplo, los que se deriven de las medidas disciplinarias adoptadas o de la exigencia de responsabilidad contractual a los auditores).

Este plazo se encuentra, según se indica en la consulta, expresamente previsto para el funcionamiento del sistema, por lo que el mismo respetaría el principio de conservación.

VII

En otro orden de cosas, y como ya se ha adelantado con anterioridad, el sistema creado deberá garantizar, en todo caso, el ejercicio de los derechos establecidos en la Ley Orgánica 15/1999, tanto en cuanto a la información que deberá facilitarse en los correspondientes contratos, como en cuanto a la información específica referida al tratamiento de los datos y el posible ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición cuando proceda.

En relación con el deber de información al denunciado, el documento WP117 señala lo siguiente:

> *"El artículo 11 de la Directiva 95/46/CE exige que se informe a las personas siempre que los datos personales se recaben de un tercero y no de ellas directamente.*
>
> *La persona acusada en el informe de un denunciante, deberá ser informada por la persona a cargo del programa tan pronto como sea posible después de que los datos relativos a ella hayan sido registrados. En virtud del artículo 14, también tendrán derecho a oponerse al tratamiento de sus datos si la legitimidad del tratamiento se basa en el artículo 7(f). No obstante, este derecho de oposición sólo podrá ejercerse en base a fundamentos legítimos relativos a la situación particular de la persona.*
>
> *En concreto, el empleado en cuestión deberá ser informado de: [1] la entidad responsable del programa de denuncia de irregularidades, [2] los hechos de los que se le acusa, [3] los departamentos y servicios que podrían recibir el informe dentro de su propia sociedad o en otras entidades o sociedades del grupo del que forma parte su sociedad, y [4] cómo ejercer sus derechos de acceso y rectificación.*
>
> *No obstante, cuando exista un riesgo importante de que dicha notificación pondría en peligro la capacidad de la sociedad para investigar de manera eficaz la alegación o recopilar las pruebas necesarias, la notificación a la persona incriminada podría retrasarse mientras exista dicho riesgo. El objetivo de esta excepción a la norma dispuesta en el artículo 11 consiste en preservar las pruebas evitando su destrucción o alteración por la persona incriminada. Deberá aplicarse de manera restrictiva, caso por caso, y deberá tener en cuenta los intereses más amplios en juego."*

En relación con este último párrafo, debe indicarse que la demora en la información al afectado no debería en ningún caso sobrepasar el plazo de tres meses previsto en el artículo 5.4 de la Ley Orgánica 15/1999, dado que nos encontramos ante un supuesto de tratamiento de datos no obtenidos del afectado.

De este modo, conforme al citado precepto, el denunciado deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del artículo 5.1 de la Ley Orgánica 15/1999.

La consulta prevé tanto la información a los empleados, que deberá canalizarse a partir de los correspondientes contratos, a fin de garantizar el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999. Asimismo, se prevé la información al denunciado de los extremos necesarios para el cumplimiento de este deber, debiendo recordarse la necesidad de que dicha información sea facilitada como máximo en el plazo de tres meses desde la presentación de la denuncia.

VIII

Por otra parte, debe señalarse por último que la sociedad que establezca los mecanismos descritos deberá implantar sobre los mismos las medidas de seguridad establecidas por el Real Decreto 994/1999, de 11 de junio.

En este punto, la consulta prevé la adopción de las medidas de seguridad de nivel básico.

No obstante, debe tenerse en cuenta lo indicado por el documento WP117, reproducido en otros lugares del presente informe, en el sentido del descrédito que puede suponer para el denunciado la inclusión de sus datos en el sistema de denuncias. Por otra parte, no es posible conocer a priori el contenido real del fichero, dado que los datos derivados de las investigaciones y averiguaciones llevadas a cabo puede implicar la inclusión en el sistema de datos especialmente protegidos, regulados por el artículo 7 de la Ley Orgánica.

En particular, dada la obligación de comunicación de los procedimientos abiertos a los trabajadores al sindicato al que el mismo se encuentren afiliados, utilización de los datos que la Agencia consideró lícita en su informe de 27 de diciembre de 2002, es posible que en caso de encontrarse el denunciado afiliado a un sindicato se incluyan en el fichero los datos vinculados a dicha afiliación sindical.

Finalmente, es también posible que el sistema incluya datos relacionados con la salud de las personas, dada la naturaleza del sector de

actividad de la consultante, perteneciente a la industria farmacéutica, pudiendo encontrarse la denuncia vinculada a situaciones relacionadas, por ejemplo, con la realización de ensayos clínicos de medicamentos.

Todo ello parece conllevar la necesaria implantación de las medidas de seguridad de nivel alto previstas en el mencionado Real Decreto 994/1999.

IX

Por último, será preciso que se proceda a notificar el tratamiento a fin de obtener su inscripción en el Registro General de Protección de Datos, así como solicitar, en su caso, la autorización para la transferencia internacional de datos que pretende realizarse a Japón, país que no ofrece un nivel adecuado de protección de datos, conforme a lo exigido por el artículo 33.1 de la Ley Orgánica 15/1999.

X

A la vista de todo ello, se considera necesario que el sistema planteado se ajuste a lo señalado a lo largo del presente informe. En particular, será precisa una aclaración de los supuestos o casos que podrán ser objeto de denuncia, en los términos mencionados en este informe, siendo la expresión empleada en la consulta sumamente amplia.

Al propio tiempo, será preciso que el sistema incluya los datos del denunciante, sin perjuicio del necesario deber de confidencialidad respecto de los mismos y de que no sean comunicados al denunciado salvo en los supuestos mencionados en la consulta.

Por último, deberían implantarse las medidas de seguridad de nivel alto.