00195/06/ES

WP 117

Dictamen 1/2006 relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios

Adoptado el 1 de febrero de 2006

ÍNDICE

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,[1]

Vistos los artículos 29 y 30(1) (c) y (3) de dicha Directiva,

Visto su Reglamento interno, y en particular los artículos 12 y 14 del mismo,

HA APROBADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

El presente dictamen proporciona directrices para la aplicación de los sistemas de denuncia de irregularidades internos de acuerdo con las normas sobre protección de datos de la UE previstas en la Directiva 95/46/CE[2].

La cantidad de cuestiones que planteó la aplicación de los sistemas de denuncia de irregularidades en Europa en 2005, incluidas las cuestiones sobre protección de datos, pone de manifiesto que el desarrollo de esta práctica en todos los países de la UE puede enfrentarse a considerables dificultades. Estas dificultades se deben en gran parte a las diferencias culturales, que se derivan a su vez de razones sociales e históricas que no pueden negarse ni obviarse.

El Grupo de Trabajo es consciente de que estas dificultades están relacionadas en parte con el gran abanico de asuntos que pueden comunicarse a través de los sistemas de denuncia de irregularidades internos. También es consciente de que los sistemas de denuncia de irregularidades plantean dificultades específicas en algunos países de la UE por lo que se refiere a aspectos de Derecho laboral, y de que se está trabajando en estos aspectos, que requerirán mayor atención. El Grupo de Trabajo también debe tener en cuenta el hecho de que en algunos países de la UE el funcionamiento de los sistemas de denuncia de irregularidades está regulado por la ley, mientras que en la mayoría de los países de la UE no existe ninguna normativa específica al respecto.

Como consecuencia, el Grupo de Trabajo considera prematuro adoptar de momento un dictamen final relativo a la denuncia de irregularidades en general. Con la aprobación del presente dictamen, el Grupo ha decidido abordar los problemas que necesitan con más urgencia directrices de la UE. Habida cuenta de esto, y por las razones que se mencionan en el documento, el presente dictamen se limita formalmente a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra el soborno y delitos financieros y bancarios.

---

1 DO L 281 de 23.11.1995, p. 31, disponible en : http://europa.eu.int/comm/internal_market/privacy/law_en.htm

2 De conformidad con el mandato específico del Grupo de Trabajo, el presente documento de trabajo no aborda otras dificultades jurídicas que plantean los sistemas de denuncia de irregularidades, en especial respecto del Derecho laboral y el Derecho penal.

El Grupo de Trabajo ha aprobado el presente dictamen entendiendo que debe seguir reflexionando sobre la posible compatibilidad de las normas relativas a la protección de datos de la UE con los sistemas de denuncia de irregularidades internos en otros ámbitos distintos a los mencionados, como por ejemplo los recursos humanos, la salud y seguridad de los trabajadores, el daño o la amenaza de daño al medio ambiente y la comisión de delitos. El Grupo proseguirá su análisis durante los próximos meses para determinar si también se necesitan directrices de la UE en estos ámbitos, en cuyo caso los principios desarrollados en el presente documento podrán complementarse o adaptarse en un documento posterior.

II. JUSTIFICACIÓN DEL ÁMBITO LIMITADO DEL DICTAMEN

La ley Sarbanes-Oxley (SOX) fue adoptada por el Congreso de los EE.UU. en 2002 a raíz de diversos escándalos financieros protagonizados por empresas.

La SOX exige que las empresas públicas de los EE.UU. y sus filiales en la UE, así como las empresas no estadounidenses que cotizan en bolsa en los EE.UU., establezcan, en su comité de auditoría, *"procedimientos para la recepción, conservación y tramitación de las denuncias recibidas por el emisor relativas a la contabilidad, las auditorías internas o las cuestiones de auditoría; así como para la presentación confidencial y anónima por parte de los empleados del emisor de situaciones relativas a cuestiones de contabilidad o auditoría cuestionables"*[3]. Además, el artículo 806 de la SOX establece una disposición dirigida a garantizar la protección de los empleados de empresas que cotizan en bolsa que proporcionen pruebas de fraude frente a las represalias que pudieran tomarse contra ellos por hacer uso del sistema de denuncia[4]. La Comisión de Valores y Cambio (SEC) es la autoridad estadounidense responsable de controlar la aplicación de la SOX.

Estas disposiciones están reflejadas en las normas del Nasdaq[5] y de la Bolsa de Nueva York (NYSE)[6]. Las empresas que cotizan en el Nasdaq o la NYSE deben certificar anualmente sus cuentas ante estos mercados. Este proceso de certificación implica que las empresas están en condiciones de afirmar que cumplen con diversas normas, incluidas las normas sobre denuncia de irregularidades.

Las empresas que no cumplen con estos requisitos de denuncia de irregularidades están sujetas a fuertes sanciones y multas por parte de Nasdaq, NYSE o SEC. A consecuencia de la incertidumbre respecto a la compatibilidad de los sistemas de denuncia de irregularidades con las normas sobre protección de datos de la UE, las empresas afectadas se enfrentan al riesgo de ser sancionadas por las autoridades de protección de datos de la UE si no cumplen las normas sobre protección de datos de la UE, y por las autoridades de los EE.UU. si no cumplen las normas de los EE.UU.

---

3 Ley Sarbanes-Oxley, artículo 301(4).

4 La ley Sarbanes-Oxley en su artículo 406, y más particularmente, las normas de las principales instituciones de valores de los EE.UU. (NASDAQ, NYSE) también establecen que las empresas que cotizan en estos mercados deben adoptar "códigos éticos" aplicables a los directivos financieros superiores por lo que respecta a asuntos de contabilidad, información y auditoría, que deben prever mecanismos de ejecución.

5 Norma 4350 (D)(3): "Responsabilidades y autoridad del Comité de Auditoría"

6 Bolsa de Nueva York (NYSE), artículo 303A.06: "Comité de Auditoría"

La aplicabilidad de algunas disposiciones de la SOX a las filiales europeas de empresas estadounidenses y a las empresas europeas que cotizan en los mercados de valores de los EE.UU. está siendo actualmente objeto de control judicial en Estados Unidos[7]. A pesar de esta incertidumbre relativa en cuanto a la aplicabilidad de todas las disposiciones de la SOX a las empresas establecidas en Europa, las empresas que están sujetas a la SOX en virtud de disposiciones extraterritoriales claras de esta ley también quieren estar en condiciones de cumplir con las disposiciones específicas sobre denuncia de irregularidades de la SOX.

Debido al riesgo de sanciones a que se enfrentan las empresas de la UE, el GT29 ha considerado urgente centrar su análisis fundamentalmente en los sistemas de denuncia de irregularidades establecidos para la comunicación de posibles violaciones de la legalidad en materia contable, de auditoría y de control de auditoria interna, según lo previsto en la ley Sarbanes-Oxley, y en cuestiones conexas que se mencionan *infra*. De esta manera, el Grupo de Trabajo se propone contribuir a la seguridad jurídica de las empresas que están sujetas tanto a las normas de protección de datos de la UE como a la SOX.

III. ESPECIAL ÉNFASIS DE LAS NORMAS SOBRE PROTECCIÓN DE DATOS EN LA PROTECCIÓN DE LA PERSONA INCRIMINADA A TRAVÉS DE UN SISTEMA DE DENUNCIA DE IRREGULARIDADES

Los sistemas internos de denuncia de irregularidades se establecen generalmente como respuesta a la necesidad de aplicar principios adecuados de gobernanza en el funcionamiento diario de las empresas. La denuncia de irregularidades se concibe como un mecanismo adicional para que los empleados comuniquen internamente las irregularidades a través de un canal específico. Este mecanismo complementa el sistema regular de información y comunicación de la organización, compuesto por los representantes de los empleados, los responsables jerárquicos, el personal de control de calidad o los auditores internos cuya misión específica es informar acerca de las irregularidades. La denuncia de irregularidades debería considerarse un sistema subsidiario y no sustitutivo de la gestión interna.

El Grupo de Trabajo subraya que los sistemas de denuncia de irregularidades deben aplicarse de conformidad con las normas sobre protección de datos de la UE. De hecho, la aplicación de los sistemas de denuncia de irregularidades, en la gran mayoría de los casos, se basará en el tratamiento de datos personales (es decir, en la recogida, registro, almacenamiento, revelación y destrucción de datos relacionados con una persona identificada o identificable), lo que significa que son aplicables las normas sobre protección de datos.

La aplicación de estas normas tendrá distintas consecuencias en el establecimiento y la gestión de los sistemas de denuncia de irregularidades. Todas estas consecuencias se detallan más adelante en este documento (véase la sección IV).

---

[7] El tribunal de apelación de los EE.UU. (1st Circuit) manifestó el 5 de enero de 2006 que las disposiciones de la SOX sobre protección de los denunciantes no se aplican a los ciudadanos extranjeros que trabajan fuera de los EE.UU. para filiales extranjeras de empresas que deban cumplir el resto de las disposiciones de la SOX.

El Grupo de Trabajo observa que, si bien la normativa y las directrices existentes sobre denuncia de irregularidades tienen como objeto prever una protección específica para la persona que utiliza el sistema de denuncia de irregularidades (el denunciante), nunca mencionan en particular la protección de la persona denunciada, en especial por lo que se refiere al tratamiento de sus datos personales. Sin embargo, incluso habiendo sido denunciado, un individuo tiene derecho a los beneficios que le conceden la Directiva 95/46/CE y las disposiciones correspondientes del Derecho nacional.

Aplicar las normas sobre protección de datos de la UE a los sistemas de denuncia de irregularidades supone dar una consideración específica a la cuestión de la protección de la persona que puede verse incriminada en una denuncia. A este respecto, el Grupo de Trabajo subraya que los sistemas de denuncia de irregularidades implican un riesgo muy grave de estigmatización y persecución de esa persona en la organización a la que pertenece. Esta persona quedará expuesta a tal riesgo incluso antes de que ella misma sea consciente de que ha sido incriminada y se hayan investigado los presuntos hechos para determinar si efectivamente se han producido.

El Grupo de Trabajo opina que la correcta aplicación de las normas sobre protección de datos a los sistemas de denuncia de irregularidades contribuirá a paliar los riesgos mencionados. También considera que, lejos de impedir que estos sistemas funcionen de acuerdo con el objeto previsto, la aplicación de estas normas contribuirá en general al correcto funcionamiento de los sistemas de denuncia de irregularidades.

IV. EVALUACIÓN DE LA COMPATIBILIDAD DE LOS SISTEMAS DE DENUNCIA DE IRREGULARIDADES CON LAS NORMAS SOBRE PROTECCIÓN DE DATOS

La aplicación de las normas sobre protección de datos a los sistemas de denuncia de irregularidades implica abordar: la cuestión de la legitimidad de los sistemas de denuncia de irregularidades (1); la aplicación de los principios de proporcionalidad y calidad de los datos (2); la información clara y completa sobre el sistema (3); los derechos de la persona incriminada (4); la seguridad de las operaciones de tratamiento (5); la gestión de los sistemas internos de denuncia de irregularidades (6); los problemas relacionados con las transferencias internacionales de datos (7); la notificación y los requisitos de comprobación previos (8).

1. Legitimidad de los sistemas de denuncia de irregularidades (artículo 7 de la Directiva 95/46/CE)

Para que un sistema de denuncia de irregularidades sea legal, el tratamiento de datos personales deberá ser legítimo y cumplir alguno de los requisitos expuestos en el artículo 7 de la Directiva sobre protección de datos.

En la situación actual, dos argumentos parecen pertinentes en este contexto: o bien el establecimiento de un sistema de denuncia de irregularidades es necesario para el cumplimiento de una obligación jurídica [letra c) del artículo 7], o bien 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 [letra f) del artículo 7][8].

i) Establecimiento de un sistema de denuncia de irregularidades necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento [letra c) del artículo 7]

El establecimiento de un sistema de información deberá tener por objeto cumplir una obligación jurídica impuesta por una norma comunitaria o de un Estado miembro, y más específicamente una obligación jurídica concebida para establecer procedimientos de control interno en áreas bien definidas.

Actualmente, tal obligación existe en la mayoría de los Estados miembros de la UE en el sector bancario, por ejemplo, donde los Gobiernos han decidido reforzar el control interno, en especial por lo que se refiere a las actividades de las sociedades de inversiones y de crédito.

La obligación jurídica de establecer mecanismos de control reforzados también existe en el contexto de la lucha contra la corrupción, en particular como consecuencia de la aplicación en el Derecho nacional del Convenio de Lucha contra la Corrupción de Agentes Públicos Extranjeros en las Transacciones Comerciales Internacionales (Convenio de la OCDE de 17 de diciembre de 1997).

Por el contrario, una obligación impuesta por una norma extranjera que exija el establecimiento de sistemas de información puede no constituir una obligación jurídica en virtud de la cual se legitime el tratamiento de datos en la UE. Cualquier otra interpretación facilitaría el que las normas extranjeras burlaran las normas comunitarias establecidas en la Directiva 95/46/CE. Como consecuencia, las disposiciones sobre denuncia de irregularidades de la SOX no pueden considerarse una base legítima para el tratamiento en virtud de la letra c) del artículo 7.

Sin embargo, en algunos países de la UE deberán establecerse sistemas de denuncia de irregularidades a través de obligaciones jurídicamente vinculantes de Derecho nacional en los mismos ámbitos que los cubiertos por la SOX.[9] En otros países de la UE donde no existen tales obligaciones jurídicamente vinculantes, podrá lograrse el mismo resultado en virtud de la letra f) del artículo 7.

---

[8] Las empresas deberán ser conscientes de que, en algunos Estados miembros, el tratamiento de datos relativos a presuntos delitos está sujeto a otras condiciones específicas relativas a la legitimidad de su tratamiento (véase *infra*, sección IV, 8).

[9] Código holandés de gobernanza empresarial, 9.12.2003, sección II, 1.6.
Proyecto español de código unificado sobre gobernanza de empresas que cotizan en bolsa, capítulo IV, 67(1)d). Este Código está pendiente de examen por la Autoridad española de protección de datos a efectos de considerar las repercusiones en la protección de datos.

ii) Establecimiento de un sistema de denuncia necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento [letra f) del artículo 7]

El establecimiento de sistemas de información puede resultar 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 [letra f) del artículo 7]. Tal razón solamente sería aceptable "siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado".

Las principales organizaciones internacionales, incluidas la UE[10] y la OCDE[11], han reconocido la importancia de establecer principios correctos de gobernanza empresarial para garantizar el adecuado funcionamiento de las organizaciones. Los principios o directrices desarrollados en estos foros consisten en una mayor transparencia, el desarrollo de buenas prácticas financieras y contables, y por tanto la mejora de la protección de los accionistas y la estabilidad financiera de los mercados. Estas organizaciones reconocen específicamente el interés de una organización en establecer procedimientos adecuados que permitan a los empleados comunicar al comité de auditoría las irregularidades y las prácticas contables o de auditoría cuestionables. Estos procedimientos de información deben garantizar la existencia de métodos para una investigación proporcionada e independiente de los hechos comunicados, que incluya un procedimiento adecuado de selección de las personas que participarán en la gestión del sistema, así como un seguimiento adecuado.

Por otra parte, estas directrices y normativas subrayan que debe garantizarse la protección de los denunciantes y que deben establecerse garantías adecuadas que protejan a los denunciantes frente a las represalias (medidas discriminatorias o disciplinarias)[12].

En efecto, el objetivo de garantizar la seguridad financiera en los mercados financieros internacionales, y en especial la prevención del fraude y las irregularidades en los ámbitos de la contabilidad, los controles de auditoría internos, las cuestiones de auditoría, la lucha contra la corrupción y los delitos financieros y bancarios o la utilización de información privilegiada, constituye un interés legítimo del empresario que justifica el tratamiento de datos personales mediante sistemas de denuncia de irregularidades en estos ámbitos. El garantizar que las denuncias sobre presuntas manipulaciones de la contabilidad o auditorías contables irregulares, que pueden tener un impacto en los estados financieros de la empresa y afectar a los intereses legítimos de los accionistas en la estabilidad financiera de la empresa, lleguen realmente a la junta directiva para ser objeto de un seguimiento adecuado, es una preocupación crítica para una empresa pública, especialmente para las que cotizan en los mercados financieros.

En este contexto, la ley Sarbanes-Oxley estadounidense puede considerarse como una de las iniciativas adoptadas para garantizar la estabilidad de los mercados financieros y la protección de los intereses legítimos de los accionistas, estableciendo normas que aseguren una gobernanza adecuada de las empresas.

---

[10] Comunidad Europea: Recomendación de la Comisión, de 15 de febrero de 2005, relativa al papel de los administradores no ejecutivos o supervisores y al de los comités de consejos de administración o de supervisión, aplicables a las empresas que cotizan en bolsa (DO L 52, 25.2.2005, p. 51).

[11] OCDE: Principios de gobernanza empresarial de la OCDE, 2004, Parte I, sección IV.

[12] Véase, por ejemplo, la *Public Interest Disclosure Act* de 1998 del Reino Unido.

Por todas estas razones, el Grupo de Trabajo considera que en los países de la UE donde no existen requisitos legales específicos que impongan la aplicación de sistemas de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios, los responsables del tratamiento de datos tienen no obstante un interés legítimo en aplicar tales sistemas internos en dichos ámbitos.

Sin embargo, 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. En especial, el artículo 14 de la Directiva 95/46/CE establece que, en los casos contemplados en la letra f) del artículo 7, el interesado tendrá derecho a oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento. Estos puntos se desarrollan a continuación.

2. Aplicación de los principios de calidad y proporcionalidad de los datos (artículo 6 de la Directiva sobre protección de datos)

De conformidad con la Directiva 95/46/CE, los datos personales deberán ser tratados de manera leal y lícita[13]; recogidos con fines determinados, explícitos y legítimos[14]; y no utilizarse para fines incompatibles. Asimismo, los datos personales deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente[15]. A veces se hace referencia al conjunto de estas normas como "principio de proporcionalidad". Finalmente, deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos sean suprimidos o rectificados[16]. La aplicación de estas normas esenciales de protección de datos tiene diversas consecuencias en cuanto a la manera en que los empleados de una organización pueden presentar denuncias y la manera en que éstas pueden ser tratadas por dicha organización. Estas consecuencias se analizan a continuación.

i) Posible límite en cuanto al número de personas autorizadas a denunciar supuestas irregularidades o malas conductas a través del sistema de denuncia de irregularidades

En aplicación del principio de proporcionalidad, el Grupo de Trabajo recomienda que la empresa responsable del sistema de denuncia de irregularidades evalúe cuidadosamente si procede limitar el número de personas autorizadas para denunciar supuestas irregularidades a través del sistema de denuncia de irregularidades, en especial habida cuenta de la gravedad de los presuntos hechos que se comuniquen. El Grupo de Trabajo reconoce, sin embargo, que las categorías de personal enumeradas pueden incluir a veces a todos los empleados en algunos de los ámbitos cubiertos por el presente dictamen.

---

13 Artículo 6(1) (a) de la Directiva 95/46/CE

14 Artículo 6(1) (b) de la Directiva 95/46/CE

15 Artículo 6(1) (c) de la Directiva 95/46/CE

16 Artículo 6(1) (d) de la Directiva 95/46/CE

El Grupo de Trabajo es consciente de que las circunstancias de cada caso serán decisivas. Así pues, no quiere ser preceptivo en este punto y deja a los responsables del tratamiento, con la eventual verificación por parte de las autoridades competentes, la competencia de determinar si tales restricciones son apropiadas en las circunstancias específicas en que se dan.

ii) Posible límite en cuanto al número de personas que pueden ser incriminadas a través de un sistema de denuncia de irregularidades

En aplicación del principio de proporcionalidad, el Grupo de Trabajo recomienda que la empresa que establezca un sistema de denuncia de irregularidades evalúe cuidadosamente si es preciso limitar el número de personas que pueden ser denunciadas en virtud del sistema, en especial habida cuenta de la gravedad de los presuntos delitos denunciados. El Grupo de Trabajo reconoce, sin embargo, que las categorías de personal enumeradas pueden incluir a veces a todos los empleados en algunos de los ámbitos cubiertos por el presente dictamen.

El Grupo de Trabajo es consciente de que las circunstancias de cada caso serán decisivas. Así pues, no quiere ser preceptivo en este punto y deja a los responsables del tratamiento, con la eventual verificación por parte de las autoridades competentes, la competencia de determinar si tales restricciones son apropiadas en las circunstancias específicas en que se dan.

iii) Fomento de las denuncias identificadas y confidenciales frente a las denuncias anónimas

Atención específica merece la cuestión de si los sistemas de denuncia de irregularidades deben permitir presentar denuncias de forma anónima en vez de abiertamente (es decir, identificándose, y en todo caso en condiciones de confidencialidad).

El anonimato puede no ser una buena solución, tanto para el denunciante como para la organización, por varias razones:

- el hecho de presentar una denuncia anónima no impide que los demás acierten al conjeturar quién presentó la denuncia;
- es más difícil investigar la denuncia si no se pueden hacer preguntas de seguimiento;
- es más fácil organizar la protección del denunciante contra las represalias, especialmente si tal protección está prevista por la ley[17], en el caso de que las denuncias se planteen abiertamente;
- las denuncias anónimas pueden llevar a la gente a centrarse en el denunciante, quizá sospechando que la denuncia se ha planteado maliciosamente;
- una organización corre el riesgo de desarrollar una cultura de recibir denuncias anónimas maliciosas;
- el ambiente de la organización puede deteriorarse si los empleados piensan que a través del sistema se pueden presentar denuncias anónimas sobre ellos en cualquier momento.

[17] Por ejemplo, la *Public Interest Disclosure Act* del Reino Unido.

En cuanto a las normas sobre protección de datos, las denuncias anónimas plantean un problema específico por lo que respecta al requisito básico de que los datos personales deben recogerse limpiamente. Por regla general, el Grupo de Trabajo considera que, para satisfacer este requisito, sólo las denuncias identificadas deben comunicarse a través del sistema de denuncia de irregularidades.

Sin embargo, el Grupo de Trabajo es consciente de que algunos denunciantes pueden no siempre estar en una posición o tener la disposición psicológica para presentar denuncias identificadas. También es consciente del hecho de que las denuncias anónimas son una realidad en las empresas, incluso y especialmente en ausencia de sistemas de denuncia de irregularidades confidenciales organizados, y que esta realidad no puede obviarse. El Grupo de Trabajo considera por tanto que la existencia de sistemas de denuncia de irregularidades puede dar lugar a que se presenten denuncias anónimas a través del mismo, y se tengan en cuenta, pero como excepción a la regla y con las condiciones que se exponen a continuación.

El Grupo de Trabajo considera que los sistemas de denuncia de irregularidades deben establecerse de tal manera que no fomenten la denuncia anónima como la forma habitual de presentar una denuncia. En especial, las empresas no deberían difundir el hecho de que pueden presentarse denuncias anónimas a través del sistema. Por el contrario, dado que los sistemas de denuncia de irregularidades deben garantizar la confidencialidad de la identidad del denunciante, los individuos que pretendan denunciar en el marco de un sistema de denuncia de irregularidades deberán saber que no sufrirán perjuicios debido a su acción. Por esta razón, los sistemas de denuncia de irregularidades deberán comunicar al denunciante, en el momento de establecerse el primer contacto, que su identidad se mantendrá confidencial en todas las etapas del proceso, y en especial no se revelará a terceros, a la persona incriminada o a los superiores jerárquicos del empleado. Si, a pesar de esta información, el denunciante desea mantener el anonimato, la denuncia se aceptará. También es necesario hacer que los denunciantes sean conscientes de que puede ser necesario revelar su identidad a las personas implicadas en las investigaciones o en los procedimientos judiciales posteriores iniciados a resultas de la investigación realizada por el sistema de denuncia de irregularidades.

La tramitación de denuncias anónimas debe ser objeto de especial precaución. Tal precaución requeriría, por ejemplo, el examen de la denuncia por parte del primer receptor de la misma por lo que se refiere a su admisión y a la conveniencia de que circule en el marco del sistema. También cabe considerar si las denuncias anónimas deben investigarse y tramitarse con mayor velocidad que las denuncias confidenciales, debido al riesgo de mal uso. Esta precaución especial no significa, sin embargo, que las denuncias anónimas no deban investigarse sin tener debidamente en cuenta todos los hechos del caso, como si la denuncia se hubiera realizado abiertamente.

iv) Proporcionalidad y exactitud de los datos recogidos y tratados

De conformidad con el artículo 6, apartado 1, letras b) y c), de la Directiva sobre protección de datos, los datos deben ser recogidos con fines determinados, explícitos y legítimos y deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

Dado que la finalidad del sistema de información es garantizar una gobernanza empresarial adecuada, los datos recogidos y tratados a través de un sistema de denuncias deberán limitarse a los hechos relacionados con este propósito. Las empresas que establezcan estos sistemas deberán definir claramente el tipo de información que puede denunciarse a través del sistema, limitando el tipo de información a la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios. En algunos países, la ley puede prever expresamente que los sistemas de denuncia de irregularidades se apliquen también a otras categorías de irregularidades graves que deban denunciarse en aras del interés público[18], pero el presente dictamen no se ocupa de éstos; pueden no aplicarse en otros países. Los datos personales tratados en el marco del sistema deberán limitarse a los datos estricta y objetivamente necesarios para verificar las alegaciones que se hayan realizado. Además, las denuncias deberán conservarse separadas de otros datos personales.

Cuando los hechos comunicados en el marco de un sistema de denuncia de irregularidades no se refieran a las áreas contempladas en el sistema en cuestión, podrán enviarse a las personas competentes de dicha empresa u organización, cuando estén en juego intereses vitales de la persona a la que se refieren los datos o la integridad moral de los empleados, o cuando, conforme al Derecho nacional, exista una obligación legal de comunicar la información a los organismos públicos o a las autoridades competentes del procesamiento de delitos.

v) Respeto de períodos estrictos de conservación de datos

La Directiva 95/46/CE establece que los datos personales tratados deberán ser conservados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Esto es esencial para garantizar el respeto del principio de proporcionalidad del tratamiento de datos personales.

Los datos personales tratados por un sistema de denuncia de irregularidades deberán eliminarse rápidamente, y generalmente en el plazo de dos meses tras la finalización de la investigación de los hechos alegados en la denuncia.

Estos períodos serán diferentes cuando se inicien procedimientos o medidas disciplinarias contra la persona incriminada o el denunciante en casos de denuncia falsa o difamatoria. En estos casos, los datos personales se conservarán hasta que finalicen los procedimientos y el plazo de recurso. Estos períodos de conservación estarán determinados por la ley de cada Estado miembro.

Los datos personales relativos a denuncias que la entidad responsable del tratamiento de la misma concluya que no tienen fundamento, deberán suprimirse sin demora.

Además, son aplicables las normas nacionales relativas a la conservación de datos en la empresa. Estas normas pueden en especial prever el acceso a los datos conservados y especificar los fines para los que es posible acceder a los datos, las categorías de personas que pueden tener acceso, y demás normas de seguridad pertinentes.

---

[18] Por ejemplo, la *Public Interest Disclosure Act* del Reino Unido.

3. Información clara y completa sobre el sistema (artículo 10 de la Directiva sobre protección de datos)

El requisito de una información clara y completa sobre el sistema obliga al responsable del tratamiento a informar a los interesados acerca de la existencia, finalidad y funcionamiento del sistema, los receptores de las denuncias y el derecho de acceso, rectificación y supresión de las personas denunciadas.

Los responsables del tratamiento también deberán informar del hecho de que la identidad del denunciante se mantendrá confidencial a lo largo del proceso, y que el abuso del sistema podrá dar lugar a una acción contra el autor del abuso. Por otra parte, también podrá informarse a los usuarios del sistema de que no se enfrentarán a ninguna sanción si utilizan el mismo de buena fe.

4. Derechos de la persona incriminada

El marco jurídico establecido por la Directiva 95/46/CE hace especial hincapié en la protección de los datos personales del interesado. Por consiguiente, desde el punto de vista de la protección de datos, los sistemas de denuncia de irregularidades deberán centrarse en los derechos del interesado, sin perjuicio de los derechos del denunciante. Deberá establecerse un equilibrio de intereses entre los derechos de las partes afectadas, incluidas las necesidades legítimas de investigación de la empresa.

i) Derechos de información

El artículo 11 de la Directiva 95/46/CE establece que deberá informarse al interesado cuando los datos hayan sido recabados de un tercero y no del propio interesado.

La persona denunciada deberá ser informada por el responsable del sistema lo antes posible en cuanto se hayan registrado los datos referentes a ella. De conformidad con el artículo 14, el interesado tendrá derecho a oponerse al tratamiento de sus datos si la legitimidad del tratamiento se basa en la letra f) del artículo 7. Este derecho de objeción, sin embargo, sólo podrá ejercerse por razones legítimas apremiantes relativas a la situación particular de la persona.

En especial, el empleado denunciado deberá ser informado acerca de: [1] la entidad responsable del sistema de denuncia de irregularidades; [2] los hechos de los que se le acusa; [3] los departamentos o servicios que pueden recibir la denuncia dentro de su propia empresa o en otras entidades o empresas del grupo al que pertenezca la empresa; y [4] cómo ejercer sus derechos de acceso y rectificación.

Sin embargo, cuando exista un riesgo considerable de que tal notificación pueda comprometer la capacidad de la empresa para investigar efectivamente la alegación o para recabar las pruebas necesarias, la notificación al denunciado podrá retrasarse mientras exista este riesgo. Esta excepción a la regla establecida por el artículo 11 tiene como objeto conservar pruebas, evitando su destrucción o alteración por el denunciado. Debe aplicarse restrictivamente, según cada caso, y deberá tener en cuenta los intereses mayores en juego.

El sistema de denuncia de irregularidades deberá adoptar las medidas necesarias para garantizar que no se destruya la información revelada.

ii) Derecho de acceso, rectificación y supresión

El artículo 12 de la Directiva 95/46/CE confiere al interesado la posibilidad de acceder a los datos registrados a fin de comprobar su exactitud y rectificarlos si son inexactos o incompletos, o si están desfasados (derecho de acceso y rectificación). Por consiguiente, el establecimiento de un sistema de denuncia debe garantizar el respeto de los derechos de los individuos al acceso y rectificación de los datos incorrectos, incompletos o desfasados.

Sin embargo, el ejercicio de estos derechos podrá restringirse para garantizar la protección de los derechos y libertades de otras personas participantes en el sistema. Esta restricción deberá aplicarse caso por caso.

Bajo ninguna circunstancia la persona denunciada podrá obtener del sistema información sobre la identidad del denunciante en virtud del derecho de acceso del denunciado, excepto cuando el denunciante presente maliciosamente una declaración falsa. En los demás casos, la confidencialidad del denunciante deberá garantizarse siempre.

Además, las personas interesadas tendrán derecho a rectificar o suprimir sus datos cuando el tratamiento de dichos datos no cumpla con las disposiciones de esta Directiva, en particular debido a la naturaleza incompleta o inexacta de los datos (artículo 12(b)).

5. Seguridad del tratamiento (artículo 17 de la Directiva 95/46/CE)

i) Medidas de seguridad materiales

De conformidad con el artículo 17 de la Directiva 95/46/CE, la empresa u organización responsable de un sistema de denuncia de irregularidades aplicará las medidas técnicas y de organización adecuadas para la protección de los datos cuando se recaben, se transmitan o se conserven. Su objetivo es proteger los datos contra la destrucción, accidental o ilícita, la pérdida accidental y la difusión o el acceso no autorizados.

Las denuncias podrán ser recogidas por cualquier medio de tratamiento de datos, electrónico o no. Estos medios deberán estar especializados para el sistema de denuncia de irregularidades, a fin de impedir cualquier desvío de su propósito original, y en aras de una mayor confidencialidad de los datos.

Las medidas de seguridad deberán ser proporcionadas a los fines de investigar las cuestiones que se planteen, de conformidad con las normas de seguridad de los distintos Estados miembros.

En los casos en que el sistema de denuncia de irregularidades esté gestionado por un proveedor de servicios externo, el responsable del tratamiento deberá estar vinculado por un contrato, y deberá tomar todas las medidas adecuadas para garantizar la seguridad de la información tratada en todo el proceso.

ii) Confidencialidad de las denuncias presentadas a través del sistema de denuncia de irregularidades

La confidencialidad de las denuncias es un requisito esencial para el cumplimiento de la obligación prevista por la Directiva 95/46/CE de seguridad del tratamiento.

Con el fin de cumplir el objetivo para el cual se ha establecido un sistema de denuncia de irregularidades y animar a las personas a utilizar el sistema y denunciar hechos que supongan conducta irregular o actividades ilegales de la empresa, es esencial que la persona que denuncie goce de una protección adecuada, garantizando la confidencialidad de la denuncia e impidiendo que terceras partes conozcan su identidad.

Las empresas que establezcan sistemas de denuncia de irregularidades deberán adoptar medidas adecuadas para garantizar que la identidad de los denunciantes sea confidencial y no se revele al denunciado a lo largo de la investigación. Sin embargo, si una denuncia resulta no tener fundamento y el denunciante ha realizado maliciosamente una declaración falsa, el denunciado podrá querer demandarlo por difamación, en cuyo caso la identidad del denunciante deberá comunicarse al denunciado si la legislación nacional lo permite. Las normas y principios nacionales sobre denuncia de irregularidades en el ámbito de la gobernanza empresarial también prevén que el denunciante deberá quedar protegido frente a medidas de represalia por utilizar el sistema, como medidas disciplinarias o discriminatorias adoptadas por la empresa u organización.

La confidencialidad de los datos personales deberá garantizarse en la recogida, revelación o conservación de los mismos.

6. Gestión de los sistemas de denuncia de irregularidades

Los sistemas de denuncia de irregularidades deben prever cuidadosamente la manera en que las denuncias se reciben y se tratan. El Grupo de Trabajo, si bien favorece la gestión interna del sistema, reconoce que las empresas pueden decidir recurrir a prestadores de servicios externos para que gestionen parte del sistema, principalmente la recogida de denuncias. Estos proveedores externos deberán estar vinculados por una obligación estricta de confidencialidad, y comprometerse a respetar los principios de protección de datos. Cualquiera que sea el sistema establecido por una empresa, la empresa deberá cumplir en particular los artículos 16 y 17 de la Directiva.

i) Organización interna específica para la gestión de los sistemas de denuncia de irregularidades

Deberá crearse un departamento específico en el seno de la empresa o grupo, dedicado a la gestión de las denuncias y a la organización de la investigación.

Este departamento deberá estar compuesto por personas con formación específica, en número limitado y con un vínculo contractual por lo que respecta a las obligaciones específicas de confidencialidad que deben asumir.

El sistema de denuncia de irregularidades deberá estar estrictamente separado de otros departamentos de la empresa, como el departamento de recursos humanos.

Este departamento garantizará, en la medida de lo necesario, que la información recogida y tratada se transmita exclusivamente a las personas que sean específicamente responsables, dentro de la empresa o grupo al que pertenezca la empresa, de la investigación o de la adopción de las medidas necesarias para realizar el seguimiento de los hechos denunciados. Las personas que reciban esta información se asegurarán de que la información recibida se maneje confidencialmente y esté sujeta a medidas de seguridad.

ii) Posibilidad de recurrir a proveedores de servicios externos

En los casos en que las empresas o grupos de empresas recurran a proveedores de servicios externos para la gestión de parte del sistema de denuncia de irregularidades, seguirán siendo responsables de las operaciones de tratamiento, pues dichos proveedores actúan como meros operadores de tratamiento en el sentido de la Directiva 95/46/CE.

Los proveedores externos pueden ser empresas que gestionen centros de atención telefónica o empresas o bufetes especializados en la recogida de denuncias y a veces incluso en la realización de parte de las investigaciones necesarias.

Estos proveedores externos también deberán cumplir los principios de la Directiva 95/46/CE. Garantizarán, en virtud de un contrato con la empresa en cuyo nombre gestionen el sistema, que realizarán la recogida y tratamiento de la información de conformidad con los principios previstos en la Directiva 95/46/CE, y que tratarán la información sólo para los fines específicos para los que se haya recabado. Estarán vinculados por obligaciones estrictas de confidencialidad y comunicarán la información tratada solamente a personas específicas en la empresa u organización responsables de la investigación o de la adopción de las medidas necesarias para realizar el seguimiento de los hechos denunciados. También respetarán los períodos de conservación a los que está vinculado el responsable del tratamiento. La empresa que utilice estos mecanismos, en su calidad de responsable del tratamiento de datos, deberá verificar periódicamente que los proveedores externos cumplen los principios de la Directiva.

iii) Principio de investigación en la UE de las empresas de la UE y excepciones

La naturaleza y estructura de las multinacionales supone que los hechos y resultados de las denuncias pueden tener que compartirse con un grupo más amplio, también fuera de la UE.

A la luz del principio de proporcionalidad, la naturaleza y gravedad del presunto delito deberán determinar en principio a qué nivel, y por tanto en qué país debe realizarse la evaluación de la denuncia. Por regla general, el Grupo de Trabajo opina que los grupos de empresas deben tratar las denuncias a escala local, es decir, en un país de la UE, en vez de compartir automáticamente toda la información con otras empresas del grupo.

No obstante, el Grupo de Trabajo reconoce algunas excepciones a esta regla.

Los datos recibidos a través del sistema de denuncia de irregularidades podrán comunicarse dentro del grupo si tal comunicación es necesaria para la investigación, dependiendo de la naturaleza o de la gravedad de la irregularidad denunciada, o si resulta necesario debido a la estructura del grupo. Esta comunicación se considerará necesaria para la investigación, por ejemplo, si la denuncia incrimina a un socio de otra entidad del grupo, a un miembro de alto nivel o a un directivo de la empresa afectada. En este caso los datos se comunicarán, confidencialmente y respetando principios de seguridad, al departamento competente de la entidad receptora, que proporcionará garantías equivalentes, por lo que se refiere a la gestión de las denuncias de irregularidades, a las de la organización responsable del tratamiento de dichas denuncias en la empresa de la UE.

7. Transferencias a terceros países

Los artículos 25 y 26 de la Directiva 95/46/CE se aplicarán cuando los datos personales se transfieran a un país tercero. La aplicación de las disposiciones de los artículos 25 y

26 será pertinente cuando la empresa haya confiado parte de la gestión del sistema de denuncia de irregularidades a un proveedor establecido fuera de la UE, o cuando los datos recogidos en las denuncias se distribuyan dentro del grupo, alcanzando por tanto a empresas que se encuentren fuera de la UE.

Es especialmente probable que estas transferencias se realicen en el caso de las filiales en la UE de empresas de países terceros.

En los casos en que el tercer país al que se envíen los datos no garantice un nivel de protección adecuado, según lo exigido por el artículo 25 de la Directiva 95/46/CE, los datos podrán transferirse siempre y cuando:

[1] el receptor de los datos personales sea una entidad establecida en los EE.UU. que haya suscrito el sistema de seguridad *Safe Harbor*;

[2] el receptor haya firmado un contrato de transferencia con la empresa de la UE que transfiera los datos, en virtud del cual esta última establezca salvaguardias adecuadas, por ejemplo basándose en cláusulas contractuales estándar publicadas por la Comisión Europea en sus Decisiones de 15 de junio de 2001 o 27 de diciembre de 2004;

[3] el receptor cuente con un conjunto de normas empresariales obligatorias debidamente aprobadas por las autoridades competentes en materia de protección de datos.

8. Cumplimiento de los requisitos de notificación

En aplicación de los artículos 18 a 20 de la Directiva sobre protección de datos, las empresas que establezcan sistemas de denuncia de irregularidades tendrán que cumplir con los requisitos de notificación a las autoridades nacionales de protección de datos o de verificación previa por parte de éstas.

En los Estados miembros que prevean tal procedimiento, el tratamiento podrá estar sujeto a la verificación previa de la autoridad nacional de protección de datos en la medida en que el tratamiento de datos presente un riesgo específico para los derechos y libertades de los interesados. Este puede ser el caso cuando el Derecho nacional permita el tratamiento, por parte de entidades privadas, de datos relativos a supuestas infracciones penales, en condiciones específicas, incluida la verificación previa de la autoridad nacional de supervisión competente. También puede ser el caso cuando la autoridad nacional considere que las operaciones de tratamiento pueden privar a las personas denunciadas de un derecho, un beneficio o un contrato. La evaluación de si el tratamiento debe ser objeto de verificación previa depende de la legislación nacional y de la práctica de la autoridad nacional de protección de datos.

V - CONCLUSIONES

El Grupo de Trabajo reconoce que los sistemas de denuncia de irregularidades pueden ser un mecanismo útil para ayudar a una empresa o a una organización a supervisar el cumplimiento de las normas y disposiciones relativas a su gobernanza empresarial, en especial en los ámbitos de la contabilidad, los controles de auditoría internos y las cuestiones de auditoría, así como de las disposiciones relativas a la lucha contra la corrupción, los delitos financieros y bancarios y el Derecho penal. Estos sistemas pueden ayudar a una empresa a aplicar debidamente los principios de gobernanza empresarial y a detectar hechos que afectarían a la posición de la empresa.

El Grupo de Trabajo pone de relieve que el establecimiento de sistemas de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios, a los que se refiere el presente dictamen, debe hacerse de acuerdo con los principios de protección de datos personales, según lo previsto en la Directiva 95/46/CE. Considera que el cumplimiento de estos principios ayuda a las empresas y a los sistemas de denuncia de irregularidades a garantizar el buen funcionamiento de tales sistemas. En efecto, es esencial que, a lo largo de todo el proceso de aplicación de un sistema de denuncia de irregularidades, se garantice el derecho fundamental a la protección de datos personales, tanto respecto del denunciante como del denunciado.

El Grupo de Trabajo subraya que los principios de protección de datos, según lo previsto en la Directiva 95/46/CE, deben aplicarse íntegramente a los sistemas de denuncia de irregularidades, en especial por lo que se refiere a los derechos de la persona denunciada a la información, acceso, rectificación y supresión de datos. Sin embargo, habida cuenta de los distintos intereses en juego, el Grupo de Trabajo reconoce que la aplicación de estos derechos puede ser objeto de restricción en casos muy específicos, con el objeto de alcanzar un equilibrio razonable entre el derecho a la intimidad y los intereses que persigue el sistema. Sin embargo, tales restricciones deberán aplicarse de forma limitada, en la medida en que sean necesarias para alcanzar los objetivos del sistema.

Hecho en Bruselas, a 1 de febrero de 2006

Por el Grupo de Trabajo

El Presidente
Peter Schaar