LA PROTECCIÓN DEL *WHISTLEBLOWER* TRAS LA DIRECTIVA (UE) 2019/1937. ANÁLISIS DEL NUEVO MARCO JURÍDICO DESDE LA PERSPECTIVA DEL DERECHO LABORAL, PÚBLICO, PENAL Y DE PROTECCIÓN DE DATOS

David Martínez Saldaña, Javier Abril Martínez, Enrique Rodríguez Celada y Laia Itziar Reyes Rico*

La protección del *whistleblower* tras la Directiva (UE) 2019/1937. Análisis del nuevo marco jurídico desde la perspectiva del Derecho laboral, público, penal y de protección de datos

El pasado 26 de noviembre de 2019, se publicó en el Diario Oficial de la Unión Europea la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Este trabajo pretende abordar, desde una perspectiva multidisciplinar, algunas de las principales cuestiones que plantea la citada Directiva; en concreto, se abordan tales cuestiones desde la perspectiva del Derecho laboral, del Derecho público, del Derecho penal y, finalmente, del Derecho de protección de datos.

The whistleblower's protection provided by (EU) Directive 2019/1937. Analysis of the new regulatory framework from an employment, public, criminal and data protection law perspective

On 26th November 2019, the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law was published in the Official Journal of the European Union. This text tries to deal with some key points of such Directive from a multidisciplinary approach; particularly, those key points are approached from Labor Law, Public Law, Criminal Law and, finally, Data Protection Law perspectives.

Palabras clave
Directiva Whistleblowing, Protección del denunciante, Represalias.

Key words
Directive Whistleblowing, Protection Whistleblower, Retaliation.

Fecha de recepción: 27-11-2019 *Fecha de aceptación: 01-12-2019*

"(...) *ningún deber contractual de buena fe obliga al trabajador a callar o a no difundir [es decir, a no ejercitar su derecho fundamental del art. 20.1 d)] unos hechos que son jurídicamente ilícitos y que pueden constituir una inconstitucional discriminación, amén de ser bien poco coincidentes con un orden de libertad y democracia* (…)"

Sentencia del Tribunal Constitucional (Sala Primera) 6/1988, de 21 de enero con ponencia de D. Luís Díez-Picazo y Ponce de León.

1 · CONTEXTO PREVIO A LA PUBLICACIÓN DE LA DIRECTIVA 2019/1937

1.1 · Contexto en el que se publica la Directiva y objeto de este trabajo

Alertar, denunciar, avisar, delatar o señalar incumplimientos detectados en la empresa o en la organización en la que uno trabaja no es algo nuevo. El hecho de "soplar el silbato" (traducción literal del término anglosajón *whistleblowing*) lleva entre nosotros desde tiempos inmemoriales.

Hace décadas que los diferentes ordenamientos jurídicos advirtieron de la importancia de la figura del alertador y de la necesidad de protegerlo. Señaladamente, en Estados Unidos lo hizo con precisión la Ley de Protección al Denunciante (*Whistleblower Protection Act*) en 1988, tal y como advertía la doctrina laboralista de principios de los años noventa al señalar que "(...) [hay] *que considerar como muy positivo la proliferación de normas sobre este tema —denominado «whistleblowing»— que se ha dado en Estados Unidos en las últimas dos décadas, y que no sólo tiene una dimensión legal, sino también profundas implicaciones morales, filosóficas y sociales*" (Del Rey Guanter)[1].

A finales de los años ochenta, nuestro Tribunal Constitucional ya se enfrentó a esta figura al conocer de recursos de amparo en asuntos de despido disciplinario basados en la deslealtad y abuso de confianza como consecuencia de las manifestaciones de trabajadores que denunciaron ilícitos en su empresa y a quienes se les declaró vulnerado su derecho a la libertad de informa-

* Abogados de las Áreas Fiscal y Laboral, Derecho Público, Procesal y Arbitraje, y Mercantil de Uría Menéndez (Madrid).

1 Salvador del Rey Guanter: *Libertad de expresión e información y contrato de trabajo*, Madrid: Civitas, 1994, pág. 100 y ss.

Martínez Saldaña, David; Abril Martínez, Javier; Rodríguez Celada, Enrique; Reyes Rico, Laia Itziar: "La protección del *whistleblower* tras la Directiva (UE) 2019/1937. Análisis del nuevo marco jurídico desde la perspectiva del Derecho laboral, público, penal y de protección de datos", *Actualidad Jurídica Uría Menéndez*, 53, 2019, pp. 24-68 (ISSN: 1578-956X).

ción —artículo 20.1.d) de la Constitución española (CE)—[2].

Como se analizará con detalle más adelante, la figura del *whistleblowing* y la necesidad de proteger a los delatores alcanzó de nuevo importancia con ocasión de los sonados escándalos de principios de los años 2000 en Estados Unidos (casos Worldcom, FBI y Enron). Más recientemente, los escándalos de las emisiones (Dieselgate), Luxleaks, Cambridge Analytica, etc., han llevado a la Unión Europea a la necesidad de regular esta figura y de fijar unos estándares mínimos para asegurar la protección de los denunciantes que alerten sobre materias clave para los intereses de la Unión, puesto que su valentía ayuda al mejor funcionamiento democrático y a luchar contra la corrupción, pero, obviamente, para ello necesitan un "*estatuto protector para quienes ponen en conocimiento público de estos hechos*"[3] que les proteja de represalias[4]. La dispersión normativa y los heterogéneos niveles de protección en cada país (prácticamente carente de regulación específica en España y en muchos países de la Unión Europea) han requerido la intervención legislativa a nivel comunitario para fijar un mínimo común en esta materia.

Es en este contexto en el que el pasado 16 de diciembre de 2019 entró en vigor la Directiva UE 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (la "Directiva") y que fija como plazo de transposición hasta el 17 de diciembre de 2021. En el caso de las entidades jurídicas del sector privado de entre 50 y 249 trabajadores, se fija el 17 de diciembre de 2023 como fecha en la que deben estar en vigor las normas nacionales que den cumplimiento a la obligación de establecer canales de denuncia interna[5].

Más allá de la fecha de trasposición, conviene habituarse cuanto antes a tener en cuenta la protección del denunciante, pues supone un cambio cultural relevante en la práctica empresarial que no solo afecta a la práctica de las relaciones laborales y recursos humanos. El *whistleblowing* es una materia compleja y poliédrica, con múltiples aristas y que afecta a distintas ramas del Derecho, por ejemplo, desde la contratación pública al *compliance* penal y la evitación de la responsabilidad jurídico-penal de la empresa a través de la introducción de los correspondientes canales, pasando por las obligaciones de tratamiento y custodia de los datos que se generan en su seno (limitación de acceso a esos datos, confidencialidad de su tratamiento o limitación temporal en la conservación de las denuncias) y, por supuesto, a la tutela de los derechos fundamentales (derecho a la libertad de expresión o, si se es más preciso, libertad de información, así como derecho a la tutela judicial efectiva en conexión con la garantía de indemnidad de trabajadores *whistleblowers*, etc.) en conexión con las sanciones y despidos que puedan producirse como resultado de las denuncias que pueden llevar a su declaración de nulidad por vulneración de derechos fundamentales con el aparejado derecho a la indemnización derivada de esa vulneración (daño moral y daños y perjuicios derivados, etc.)[6].

El presente artículo tiene por objeto el análisis del panorama previo a la publicación de la Directiva y el impacto de su entrada en vigor en el Derecho laboral, el Derecho público, el Derecho penal y el Derecho a la protección de datos.

1.2 · Conceptos de *whistleblowing* y *whistleblower*

El punto de partida en esta materia necesariamente debe ser la definición de *whistleblowing y whistleblower*, y la diferenciación entre ambos conceptos.

Tal y como recuerda Del Rey Guanter (1994)[7], una de las primeras definiciones del término *whistleblowing* fue acuñada por el activista y abogado estadounidense de origen libanés Ralph Nader, que trabajó durante décadas en favor del medio ambiente, de los derechos del consumidor y de la

2 Sentencia del Tribunal Constitucional (Sala Primera) 6/1988, de 21 de enero (RTC 1988, 6).

3 Patricia Nieto Rojas: "*Whistleblowers*. Aspectos laborales de la Directiva relativa a la protección de las personas que informen sobre infracciones de Derecho de la UE", *El Foro de Labos*. Disponible en https://forodelabos.blogspot.com/2019/10/whistleblowers-aspectos-laborales-de-la.html.

4 La necesidad de protección del denunciante es la principal razón de ser de la Directiva UE 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, que en su considerando primero, advierte: "[...] *los denunciantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias. En este contexto, es cada vez mayor el reconocimiento, a escala tanto de la Unión como internacional, de la importancia de prestar una protección equilibrada y efectiva a los denunciantes*".

5 Artículo 26 de la Directiva, "*Transposición y periodo transitorio*".

6 Artículo 183 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.

7 Salvador del Rey Guanter: *Libertad de expresión e información..., op. cit.,* pág. 100.

democracia. Nader (1985) definió el *whistleblowing* a mediados de los años ochenta, abandonando su connotación negativa (chivato) y tratando de darle un enfoque positivo, como "*un acto de un hombre o una mujer que, creyendo que el interés público prevalece* [sobre] *el interés de la organización en la que él o ella sirve, sopla el silbato públicamente cuando la organización está implicada en actividades corruptas, ilegales, fraudulentas o lesivas*".

En un interesante y reciente trabajo, Pérez Triviño (2018)[8] recoge algunas de las "*muchas y variadas definiciones de whistleblowing*", como la de la profesora de la Universidad de Glasgow, Marion Hersh (2002), que lo definió como "*revelación deliberada de información acerca de actividades no triviales que se creen peligrosas, ilegales, inmorales, discriminatorias o que de otra manera incluyen una infracción, generalmente por miembros actuales o pasados de la organización*"[9].

Asimismo, Pérez Triviño señala a otros autores, como Ragués (2013)[10], quien añadió que el ente en cuyo ámbito se produce la denuncia puede ser "*tanto público como privado*" y que "*la información se traslada bien a los superiores dentro de la propia organización o bien de terceras partes*", poniendo el foco en que las revelaciones pueden llevarse a cabo dentro de la propia organización, a nivel interno, o bien en canales externos. Como se verá, la Directiva plantea una clara prelación en la que, en primer lugar, deben emplearse los canales internos y, solo en determinadas circunstancias, los canales externos[11], o bien, como *ultima ratio*, la revelación pública (circunstancias que son relevantes para que el *whistleblower* esté calificado para contar con la protección que despliega la Directiva, cuestión relevante como se expondrá en el capítulo laboral —2.1.2(C)(i)—).

El propio Pérez Triviño (2018)[12] ofrece finalmente una definición de *whistleblowing*: "[...] *la revelación deliberada de información acerca de actividades no triviales que se creen peligrosas, ilegales, inmorales, discriminatorias o que de alguna otra manera incluyen una infracción en una organización, siendo tal revelación llevada a cabo por miembros actuales o pasados de la organización, que no tienen deberes de información o de vigilancia, y pudiendo ir dirigida a órganos de la propia organización o a terceras partes*".

La documentación que se generó durante la tramitación de la Directiva[13] también es de ayuda para conocer con la máxima precisión el concepto de *whistleblowing*. Así, la exposición de motivos ("*explanatory memorandum*")[14] que acompañaba a la Propuesta de la Directiva (2018)[15] definió el *whistleblowing* (procedimiento de denuncia de infracciones) como un "*medio de alimentar los sistemas de aplicación de la legislación nacional y de la UE con información que permita la detección eficaz, la investigación y el enjuiciamiento de infracciones de las normas de la Unión*" (apartado primero, párrafo cuarto, de la exposición de motivos)[16].

Probablemente, la exposición de motivos se inspiró en la Opinión 1/2006 del Grupo de Trabajo del Artículo 29, de 1 de febrero de 2006 (que se define y comenta en el apartado 2.1 y 2.4.1 de este trabajo), y que expuso que el "*whistleblowing se ha diseñado como un mecanismo adicional para que los empleados puedan denunciar incumplimientos internamente a través de un canal específico. Es un complemento de los canales de información habituales de la organización, tales como los representantes de los trabajadores, los mandos directivos, el personal de control de calidad o los auditores internos, cuya función es precisamente denunciar esos incumplimientos. El whistleblowing*

8 José Luis Pérez Triviño: "*Whistleblowing*". *Eunomía. Revista en Cultura de la Legalidad*, n.º 14, abril-septiembre 2018, pág. 286. Disponible en https://e-revistas.uc3m.es/index.php/EUNOM/article/view/4170/2694

9 M. A. Hersh: "Whistleblowers. Heroes or traitors? Individual and collective responsibility for ethical behaviour", *Annual Review in Control*, 26, 2002, págs. 234-262.

10 Ramón Ragués i Vallés: *Whistleblowing. Una aproximación al Derecho penal*, Madrid: Marcial Pons, 2013, pág. 20.

11 Es significativo, a este respecto, lo que se indica en el considerando 33 de la Directiva: "*En general, los denunciantes se sienten más cómodos denunciando por canales internos, a menos que tengan motivos para denunciar por canales externos*".

12 José Luis Pérez Triviño: "*Whistleblowing*", *op. cit.*, pág. 287.

13 Esa documentación y el proceso de tramitación de la propuesta de Directiva se analiza con detalle en David Martínez Saldaña e Ignacio Moreno Lucenilla: "La Protección del *whistleblower* y el *compliance* laboral", *Revista de Información Laboral*, nº 12, 2018.

14 Explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union Law ("Exposición de motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión").

15 Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union Law ("Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión"). Brussels, 23.4.2018. COM (2018) 218 final. 2018/0106 (COD).

16 "[...] *whistleblowing is a means of feeding national and EU enforcement systems with information leading to effective detection, investigation and prosecution in breaches of Union Rules*" (apartado primero, párrafo cuarto de la exposición de motivos).

debería verse como un complemento, y no como un sustituto, de la gestión interna".

El *whistleblowing* es, por tanto, un medio, un canal o "*sistema de información de denuncias*"[17] para revelar y hacer llegar esa información relevante sobre potenciales incumplimientos que una persona física conoce en el "*marco de sus actividades laborales*" o "*contexto laboral*". A su vez, ese "*contexto de laboral*" lo define la Directiva como las "*actividades de trabajo presentes o pasadas en el sector público o privado a través de las cuales, con independencia de la naturaleza de dichas actividades, las personas pueden obtener información sobre infracciones y en el que estas personas podrían sufrir represalias si comunicasen dicha información*" (artículo 5, apartado 9). Se trata de un alcance expansivo relevante desde la perspectiva laboral y que se analizará, conforme se ha anticipado, en el apartado 2.1 de este trabajo.

Así pues, mientras *whistleblowing* se refiere al canal, *whistleblower* es el sujeto que formula la denuncia. Ya se ha adelantado que, literalmente traducida, la expresión *whistleblower* significa "el que hace sonar el silbato", y se refiere a los policías que antiguamente realizaban dicha acción para avisar a otros agentes cuando advertían la presencia de un delincuente[18]. En castellano podría traducirse como "chivato", "soplón", o "delator", términos todos ellos muy peyorativos, cuando, si bien se mira, la Directiva refuerza esta figura como medio de apoyo al cumplimiento de la normativa de la UE y de la defensa de los valores y principios democráticos, por ejemplo, a través de la lucha contra la corrupción, cambio de orientación del concepto que ya sugirió Nader. En este sentido, se utilizan también términos más neutros y acordes con ese planteamiento, como "el que da la voz de alarma", el "informante interno" o el "denunciante".

Por un concepto similar apuesta la Directiva (2019), que define al *whistleblower* como "denunciante" ("*reporting person*"), que es "*aquella persona física que comunica o revela públicamente información sobre infracciones obtenida en el marco de sus actividades laborales*"[19] (artículo 5, apartado 7). El considerando 1 de la Directiva reflexiona acerca de los *whistleblowers* y afirma que "[...] *al dar la voz de alarma desempeñan un papel clave a la hora de descubrir y prevenir las infracciones de la ley y de proteger el bienestar de la sociedad. Sin embargo, los potenciales denunciantes suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias*".

El documento-resumen que acompañaba a la Propuesta de Directiva, denominado *Fact sheet on whistleblower protection* ("*Fact sheet*") (2018)[20], elaborado por la Comisión Europea, aporta una sencilla y práctica definición de *whistleblower*: "[...] *personas que, cuando se topan, en el contexto de su trabajo, con delitos que pueden perjudicar el interés público, por ejemplo, daños al medio ambiente, a la salud pública, a la seguridad de los consumidores y a las finanzas públicas de la UE, los revelan (y no los silencian)*".

En términos similares, el documento elaborado por la Comisión Europea, denominado *Frequently Asked Questions: Whistleblower protection* ("FAQ") (2018)[21] y que acompaña a la Propuesta de Directiva, subraya que esta última "[...] *define a los* whistleblowers *como aquellos que denuncian o revelan información sobre violaciones del Derecho de la Unión de la que han tenido conocimiento en sus actividades laborales. Esto significa que cubre a los empleados, pero también a los trabajadores autónomos, freelancers, consultores, contratistas, proveedores, voluntarios, becarios no remunerados y candidatos a puestos de trabajo*". Esta ampliación del concepto laboral, en efecto, aparece en el propio ámbito de aplicación de la Propuesta de Directiva, que pretende ser expansivo para llegar al máximo número de roles intervinientes en el contexto laboral, sin limitarse al trabajador por cuenta ajena (ámbito personal de aplicación, artículo 4 de la Directiva). Sobre esta cuestión nos remitimos al capítulo 2.1.2(A).

1.3 · Necesidad de proteger a los *whistleblowers* y ausencia de regulación completa en España y otros países de la UE

Ya se ha anticipado que el papel del *whistleblower* es relevante en una sociedad democrática, como instrumento de lucha contra las ilegalidades y la corrupción. Uno de los claros e históricos ejemplos de la utilidad de esta figura la encontramos en el

17 Expresión utilizada por el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales.

18 El origen de la expresión *whistleblower* se expone con detalle en *La protección del "whistleblower" o del "informante delator"*. Disponible en http://lexinformatica.co/2017/11/05/la-proteccion-del-whistleblower-o-del-informante-delator/.

19 "«Reporting person» means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities".

20 European Commission. Directorate-General for Justice and Consumers. *Whistleblower protection. Fact sheet*. Abril 2018.

21 European Commission. Directorate-General for Justice and Consumers. Frequently Asked Questions. 23 de abril de 2018.

caso de la empresa estadounidense de energía Enron que se reveló en octubre de 2001 y que condujo a la quiebra de esa empresa y a la disolución de la auditora Arthur Andersen. En esencia, un equipo de ejecutivos de Enron, a través del uso de lagunas de contabilidad, entidades de propósito especial e informes financieros, fueron capaces de esconder miles de millones de dólares en deudas de ofertas y proyectos fallidos. Los accionistas perdieron cerca de once mil millones de dólares cuando el precio de la acción de Enron, que llegó a un máximo de noventa dólares por acción a mediados del año 2000, se desplomó a menos de un dólar a finales de 2001. Como consecuencia del escándalo, se promulgaron nuevas regulaciones y leyes para ampliar la exactitud financiera de las compañías públicas y cotizadas. En particular, la conocida *Sarbanes-Oxley Act*[22], en su sección 806, fue una de las pioneras en buscar la protección de los empleados, tanto de empresas públicas como de cotizadas, que revelaran pruebas de fraude y necesitaran medidas de protección contra cualquier represalia derivada de haber hecho uso del canal de denuncias. En concreto, imponía la obligación, tanto a las empresas estadounidenses cotizadas como a sus filiales (incluidas las que se encontraran en España), y a las que emitieran valores en Estados Unidos, de contar con sistemas y canales de denuncia de irregularidades.

En efecto, desde ese momento, la figura del *whistleblower* empieza a considerarse de manera positiva y se toma consciencia de su necesidad de protección en Estados Unidos. Buena muestra de ello la constituye el hecho de que, en 2002, la revista *Time* otorgara la condición de "personajes del año" a tres *whistleblowers*, en concreto a la informante del caso Enron (Sherron Watkins) y a las informantes de otros dos casos muy relevantes del momento: Worldcom (Cynthia Cooper) y FBI (Coleen Rowler).

En la actualidad, la motivación para la nueva regulación de la protección del *whistleblower* que establece la Directiva bebe también de los recientes escándalos que, en muchos casos, han visto la luz gracias a personas que han denunciado la existencia de ilícitos de los que han tenido conocimiento en el contexto laboral. Así, el documento FAQ menciona el escándalo de las emisiones (Dieselgate), el escándalo Luxleaks, los papeles de Panamá y el caso Cambridge Analytica, entre otros.

De manera similar, en España se ha conocido recientemente la sentencia del caso de los ERE en Andalucía. El supuesto emergió gracias a una denuncia de un empleado de la Agencia IDEA que fue despedido como represalia por esa revelación de información y cuyo despido fue declarado nulo por la Sala de lo Social del Tribunal Superior de Justicia de Andalucía[23], con la obligación de readmisión y de abono de indemnización por vulneración de su derecho fundamental (libertad de expresión —artículo 20.1.a de la Constitución Española ("CE") y de su derecho a la tutela judicial efectiva en la vertiente de la lesión de garantía de indemnidad —artículo 24 CE—). El otro caso insignia español que vio la luz gracias a un denunciante fue el caso Gürtel. Sobre ello, el profesor Todolí Signes[24] ha señalado que "[...] *todos recordaremos el caso de Ana Garrido, la trabajadora del Ayuntamiento de Boadilla, que tras denunciar el caso Gürtel en su pueblo, tuvo que demandar al ayuntamiento por acoso laboral. En efecto, sin una protección legal eficaz, los informantes se ven totalmente desprotegidos ante las represalias de sus jefes, teniendo que recurrir a largos y costosos procedimientos ante los tribunales. Sin contar el efecto desincentivante que estas acciones pueden provocar en futuros delatores y el perjuicio al interés público que ello desencadena*".

La UE es plenamente consciente de la necesidad de protección del *whistleblower*, como se muestra en el breve y muy clarificador vídeo que se adjuntó a la nota de prensa que anunciaba la Propuesta de Directiva. Así, en su acto de presentación, el vicepresidente primero de la Comisión Europea, Frans Timmermans, expuso que "*muchos escándalos jamás habrían salido a la luz si aquellos que estaban dentro no hubieran tenido el coraje de denunciar. Pero aquellos que lo hicieron tomaron riesgos enormes. Así que si protegemos mejor a los whistleblowers, podremos detectar mejor y prevenir el daño al interés público tal como el fraude, corrupción, evasión fiscal, o daño a la salud pública y al medio ambiente*". A ello, la comisaria europea de Justicia, Vera Jourová, añadió que "[...] *la nueva regulación sobre whistleblowers va a suponer un cambio en las reglas del juego. En el mundo globali-*

22 Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 30 de julio de 2002. También conocida como la "*Ley de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista*", aunque también es llamada SOx, SarbOx o SOA.

23 Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Andalucía (Sevilla), Sección Primera, de 13 de diciembre de 2018 (N.º recurso 4378/2017).

24 Adrián Todolí Signes: "La regulación de los whistleblowers", *Agenda Pública*, *El País*, 12 de septiembre de 2015. Disponible en http://agendapublica.elpais.com/la-regulacion-de-los-whistleblowers/.

zado en el que la tentación de maximizar los beneficios a veces a expensas de la ley es real, necesitamos apoyar a la gente que está dispuesta a tomar riesgos para destapar violaciones serias del Derecho de la Unión. Se lo debemos a la gente honesta de Europa"[25].

En efecto, como expone el *Fact sheet,* los *whistleblowers* necesitan protección ante la degradación, la posibilidad de afrontar procedimientos judiciales, perder sus trabajos y su estabilidad económica, así como para defender el mantenimiento de su buen nombre y reputación. Por ello, el 81 % de los consultados en el *Eurobarómetro especial sobre corrupción* contestaron que no denunciarían actos de corrupción a los que hubieran tenido acceso. El motivo: el miedo a las consecuencias de esas denuncias. Adicionalmente, dos cuestiones más requerían de la intervención del legislador europeo: (i) en primer lugar, la falta de homogeneidad en la regulación de protección del *whistleblower* (solo diez países de la UE disponen de una ley que los proteja: Francia, Hungría, Irlanda, Italia, Lituania, Malta, Países Bajos, Eslovaquia, Suecia y Reino Unido —en España no se dispone de legislación de protección del *whistleblower* más allá de las referencias dispersas que se citan en este trabajo—)[26], además de que, a nivel europeo, se han implementado medidas, en su mayoría, limitadas al sector financiero, por lo que hace falta una homogeneización[27]; (ii) en segundo lugar, la ausencia, hasta la fecha, de sistemas de protección eficaces y homogeneizados ha hecho necesario introducir un sistema de protección garantista, que incluya el establecimiento de canales seguros para las denuncias, tanto dentro de las organizaciones privadas como en el seno de las públicas, y que logre la adecuada protección a los *whistleblowers* ante el despido, la degradación y cualquier forma de represalia, además de la formación de las autoridades públicas acerca de cómo debe atenderse a los *whistleblowers.*

2 · LA DIRECTIVA DESDE SUS DISTINTAS PERSPECTIVAS

2.1 · La Directiva desde la perspectiva laboral

2.1.1 · Panorama previo a la publicación de la Directiva

a) Importancia de la doctrina del Tribunal Constitucional en materia de libertad de expresión y libertad de información

En el ámbito laboral español, la figura del *whistleblower*, sin haber sido definida o regulada hasta la fecha, empezó a encontrar alguna protección por la vía de la invocación de la violación de los derechos fundamentales del trabajador-*whistleblower* represaliado a finales de los años ochenta. Así, en ese momento, una de las herramientas que se tenían al alcance era el derecho a la libertad de expresión (artículo 20.1.a CE), que reconoce la "*libertad de expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de producción*", aunque más preciso era y es invocar el derecho a la libertad de información (artículo 20.1.d CE), que comprende el hecho de "*comunicar o recibir libremente información veraz por cualquier medio de difusión*". Este último derecho es el que mejor se corresponde con el *whistleblower*, ya que está precisamente revelando y comunicando información. En efecto, y aunque a veces la jurisdicción social pueda declarar la nulidad del despido del *whistleblower* como consecuencia de la lesión de la libertad de expresión (por ejemplo, Sentencia de la Sala de lo Social del Tribunal Superior de Justicia del País Vasco de 12 de julio de 2005[28]), el *whistleblowing* consiste no tanto en "*expresar libremente pensamientos*", sino en "*comunicar información*", esto es, en informar, eso sí, bajo la perspectiva de la expectativa de veracidad que requiere la Directiva (artículo 6.1.a) y la CE (artículo 20.1.d).

25 Declaraciones recogidas en la nota de prensa de la Comisión Europea "Whistleblower protection: commission sets new, EU wide rules". Bruselas, 23 de abril de 2018. Disponible en https://eeas.europa.eu/delegations/india/43385/whistleblower-protection-commission-sets-new-eu-wide-rules_en.

26 No obstante, existe algún intento aislado. En concreto, una proposición de "Ley de protección integral de los alertadores" que presentó el Grupo Mixto en la XIII legislatura (*Boletín Oficial de las Cortes Generales* de 11 de junio de 2019).

27 El considerando 4 de la Directiva señala que "[...] *las consecuencias de la infracciones del Derecho de la Unión con dimensión transfronteriza sacadas a la luz por los denunciantes muestran cómo una protección insuficiente en un Estado miembro no sólo tiene un impacto negativo sobre el funcionamiento de las políticas de la UE en ese Estado, sino que puede extenderse también a otros Estados miembros y a la Unión en su conjunto*".

28 La sentencia de la Sala de lo Social del Tribunal Superior de Justicia del País Vasco de 12 de julio de 2005 (ROJ: STS PV 3244/2005) trata el caso de un trabajador despedido por comunicar al servicio de intervención de la empresa varias irregularidades en la gestión y funcionamiento de su centro de trabajo. La empresa no pudo demostrar que el despido obedeciera a una causa distinta a la represión de la denuncia del actor y, en consecuencia, la Sala declaró su nulidad. Resulta de interés aquí el razonamiento de la Sala sobre los términos y formas en los que se planteó la denuncia, que alude al derecho del trabajador a la libertad de expresión: "*Es interesante destacar que aquellas denuncias fueron internas, dentro de la empresa, en términos correctos, sin recurrir al insulto, la expresión grosera o la injuria y por tanto, sin sobrepasar los límites del ejercicio de aquel derecho* [se refiere aquí a la libertad de expresión]".

En este sentido, la doctrina científica (Guamán Hernández, 2005) 29, con apoyo en abundante doctrina del Tribunal Constitucional ("TC"), ya señaló que el derecho comprometido en los despidos de los delatores es la libertad de información, que les ampara, dado que se trata de "*comunicación de informaciones verídicas cuando las mismas revisten un interés general. En este caso y al entrar en juego la libertad de información y la formación de la opinión pública es necesario ponderar los derechos en juego*". No en vano, lo que subyace aquí como bien a proteger es la valía de la información "noticiable" que aporta el *whistleblower* para el sistema democrático, pues, como apuntaba Guamán Hernández, se trata del "*ejercicio correcto* [que] *la información tiene para el mantenimiento de la sociedad democrática*". La Directiva, en su considerando 31, hace referencia a ambos derechos —libertad de expresión e información— con cita del artículo 11 de la Carta Social Europea y del artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos, y recuerda que ella misma "*se basa en la jurisprudencia del Tribunal Europeo de Derechos Humanos ("TEDH") sobre el derecho a la libertad de expresión y en los principios desarrollados por el Consejo de Europa en su Recomendación sobre protección de denunciantes adoptada por su Comité de ministros el 30 de abril de 2014*" [30].

Una de las sentencias del TC más representativas de finales de los años ochenta que concedió el amparo como consecuencia de la vulneración del derecho a la información fue la STC 6/1988 [31]. Esta sentencia "*establece por primera vez, de manera rotunda, las diferencias entre las libertades de expresión e información*" [32] —en concreto, realiza esa diferenciación en su fundamento de derecho quinto—. Se analizaba allí el despido de un redactor de la Oficina de Prensa del Ministerio de Justicia por deslealtad, al haber manifestado su "*preocupación por la filtración de noticias desde ese Departamento a la Editorial PRISA dado que* [...] *esas noticias afectan a todos los ciudadanos españoles*". El despido se declaró nulo al concederse el amparo por vulneración de derechos fundamentales. Se consideró que ese acto debía considerarse como un ejercicio de libertad de información, que no de libertad de expresión, y se argumentó que no son dos derechos "*fáciles de separar*" de modo que cuando "*puedan aparecer entremezclados*" habrá que atender "*al elemento que en ellos aparece como preponderante*", que en este caso fue la comunicación "*de hechos que pueden considerarse noticiables*" (fundamento de derecho quinto de la STC 6/1988). El TC aplicó el triple canon para determinar si el derecho a la libertad de información se ejercitó correctamente, y concluyó que (i) la información reunía el requisito de veracidad [33];(ii) se había empleado el medio adecuado ("*información rectamente obtenida y difundida*"); y que (iii) existía relevancia pública en la información emitida.

Es importante señalar que estos tres elementos que aparecen en la doctrina del TC de finales de los años ochenta también encuentran su reflejo en la Directiva, dado que (i) se exige al denunciante que, para poder tener derecho a la protección, tenga "*motivos razonables para pensar que la información sobre infracciones denunciadas es veraz en el momento de la denuncia y que la citada información entra dentro del ámbito de aplicación de la Directiva*" (por tanto, no se exige veracidad absoluta, sino una expectativa de veracidad); (ii) se exige también que se empleen los canales de manera adecuada, esto es, los internos en primer lugar, en segundo lugar los externos y, en

29 Adoración Guamán Hernández: *La libertad de información del trabajador. Doctrina constitucional*, Valencia: Tirant lo Blanch, 2005, pág. 84.

30 Conviene destacar, por su interés, la Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala, caso Guja contra Moldavia, demanda núm. 14277/04, de 12 de febrero de 2008 (ECLI:CE:ECHR:2008:0212JUD001427704). Se analizaba aquí el caso de un empleado de la Fiscalía General moldava que fue despedido por haber divulgado en prensa documentos que revelaban las injerencias de un alto cargo político en un procedimiento penal. Como fundamento de la demanda, el actor alega que el cese viola su derecho a la libertad de expresión, y que la divulgación de los documentos tenía como propósito luchar contra la corrupción y el tráfico de influencias. El Tribunal argumenta que "*La divulgación al público no debe considerarse más que como último recurso, en caso de imposibilidad manifiesta de actuar de otro modo* [...]", y que, ante la inexistencia de medios internos alternativos y la importancia que tiene esa información para el interés de la opinión pública, "*la divulgación* [...] *a un periódico podría justificarse*". De nuevo, aparece la "revelación pública" y el interés público en conocer esa información oculta como bien jurídico protegido que justifica la protección del *whistleblower* (por ejemplo, considerandos 31 y 33 de la Directiva). Además, el Tribunal razona que el grado de protección se modula en razón de la buena fe del denunciante, la convicción de que la información es auténtica (de nuevo, la expectativa de veracidad) y la inexistencia de medios alternativos. Esta sentencia fue tenida en cuenta en la elaboración de la Propuesta de Directiva, como así lo señalaba su considerando 57.

31 STC 6/1988, de 21 de enero de 1988 (ECLI:ES:TC:1988:6).

32 Adoración Guamán Hernández: *La libertad de información del trabajador...*, *op. cit.*, pág. 88.

33 Aunque no se exige una veracidad absoluta, pues su "total exactitud puede ser controvertible", sino que lo que se exige es un deber de diligencia del informador, a quien se le puede y debe exigir que lo que transmita como «hechos» haya sido objeto de previo contraste con datos objetivos, privándose, así, de la garantía constitucional a quien, defraudando el derecho de todos a la información, actúe con menosprecio de la verdad o falsedad de lo comunicado —fundamento de derecho quinto de la STC 6/1998—)

tercer lugar, la revelación pública a los medios —artículo 6.1.b en relación con los artículos 7 a 15 de la Directiva— (por tanto, la información debe ser rectamente difundida); y (iii) se exige que el contenido del mensaje tenga relevancia pública, dado que tiene que referirse a lo que los considerandos de la Directiva han definido como intereses esenciales de la Unión, esto es, contratación pública, servicios, productos y mercados financieros, prevención del blanqueo de capitales, seguridad de los productos, del transporte, protección del medio ambiente frente a radiaciones y seguridad nuclear, seguridad de los alimentos, piensos y seguridad animal, salud pública, protección de los consumidores y protección de la privacidad, datos personales y seguridad en las redes y sistemas de información (por tanto, el interés público en la información emitida). En definitiva, la relevancia pública la pone de manifiesto el ámbito de aplicación material de la Directiva (artículo 2 de la Directiva), y conviene recordar que la protección al denunciante requiere que la información que revela verse sobre estas materias (artículo 6.1.a de la Directiva).

A esta doctrina del TC (sentencia 6/1998) se refiere la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Andalucía (Sevilla), Sección Primera, de 13 de diciembre de 2018 (N.º recurso 4378/2017), en la que se juzgaba el ya mencionado despido de un trabajador *whistleblower* que sacó a la luz el caso de los ERE. La sentencia expone que "*queda así probado que voluntariamente y por los conocidos hechos* [...] *de la declaración que efectuó en el procedimiento de investigación penal en el llamado caso de los EREs, se optó por denegar el reconocimiento de la excedencia forzosa al actor y su despido* [...]. *En fin, como la demandada no acreditó una justa causa y razonable en el cese, se acredita que el despido trae casusa de una represalia por ejercitar derechos*". Esta sentencia consideró que el despido obedeció a móviles discriminatorios y que conculcó el principio de igualdad, la libertad ideológica, la libertad de expresión y la garantía de indemnidad por sus reiteradas demandas y por su testimonio en un procedimiento penal, aunque se echó en falta una declaración más precisa de la vulneración del derecho a la libertad de información.

Igualmente, la doctrina del TC (sentencia 6/1998) ha sido recientemente citada por una interesante sentencia del TC dictada precisamente la víspera de que se publicase la Directiva. En concreto, se trata de la sentencia 146/2019, de 25 de noviembre de 2019[34]. El *whistleblower*, en este caso, es un enfermero que trabajaba para la empresa contratista del servicio de gestión del centro de día de Baracaldo, centro del que es titular el Ayuntamiento de esta localidad.

El trabajador formuló una serie de quejas ante su empleadora, la empresa adjudicataria, en el sentido de cuestionar la profesionalidad, la calidad del servicio, la falta de material sanitario y otros medios en el centro, la preparación del personal e incluso un incidente sobre un riesgo de contagio de hepatitis B (antecedente 2.a de la sentencia 146/2019). Posteriormente, "desatendidas sus reivindicaciones" formuladas ante la empresa adjudicataria, el trabajador denunció estos hechos directamente ante el Ayuntamiento (por tanto, el cliente de su empleadora). Como consecuencia de ello, se procede a su despido disciplinario por ser contrario a la "buena fe contractual" y al "deber de lealtad", y se imputa específicamente la revelación al Ayuntamiento como incumplimiento en la carta de despido (de modo que no hay duda de que existe una conexión entre la denuncia y el despido).

El trabajador impugnó el despido, que fue declarado nulo en la instancia por sentencia del Juzgado de lo Social núm. 7 de Bilbao, de 16 de diciembre de 2015 (al entender el que existió una vulneración del derecho a la libertad de expresión), e improcedente en la Sala de lo Social del Tribunal Superior de justicia del País Vasco, por sentencia de 10 de mayo de 2016 (que estimó el recurso de suplicación al entender que no estaba comprometido el derecho a la libertad de expresión porque planteó sus reivindicaciones laborales "por cauce inadecuado" y "se inmiscuyó en denuncias para las que no estaba legitimado y que por no haber quedado acreditadas fueron meras apreciaciones cuya sola mención ante el Ayuntamiento causaron a la empresa un perjuicio injusto").

Contra la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia del País Vasco se interpuso recurso de casación para la unificación de la doctrina ante la Sala de lo Social del Tribunal Supremo, y se adujo como sentencia de contraste

34 Un comentario a esta sentencia puede encontrarse en David Martínez Saldaña: "El Tribunal Constitucional otorga el amparo a un "proto-whistleblower" (la STC 146/2019, de 25 de noviembre, como contrapunto a la STC 126/2003, de 30 de junio)", El Foro de Labos. Disponible en https://forodelabos.blogspot.com/2020/01/el-tribunal-constitucional-otorga-el.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+ElForoDeLabos+%28El+Foro+de+Labos%29.

la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Cataluña de 31 de octubre de 2012 a la que se ha referido el profesor Rojo Torrecilla en su comentario de la STC 146/2019[35]. Resulta de interés esta sentencia al abordar el caso de un trabajador *whistleblower* que prestaba servicios en una empresa adjudicataria del servicio de gestión del alumbrado público en favor del Ayuntamiento de Barcelona y que cursó centenares de quejas durante dos meses, y lo hizo directamente ante el Ayuntamiento a través del portal de internet de atención al ciudadano en relación con el servicio prestado por la empresa para la que trabajaba. La empresa adjudicataria de ese servicio para la que trabajaba le despidió por considerar las quejas altamente perjudiciales y por haberse llevado a cabo con transgresión de la buena fe contractual por no haberlas cursado con anterioridad a través de los canales jerárquicos empresariales y al objeto de haber podido solucionar aquellas que realmente fueran ciertas. La Sala de lo Social del Tribunal Supremo no apreció contradicción y desestimó el recurso de casación para la unificación de la doctrina.

Ante ello, se recurrió al TC en amparo. El TC otorgó el amparo al *whistleblower* en la sentencia y lo hizo identificando previamente que podría haber existido una represalia y, por tanto, una lesión del derecho a la tutela judicial efectiva (24 CE) a la que no puede atender por no haberse alegado en el recurso de amparo, dado que no es "*tarea de este Tribual reconstruir la demanda de oficio para suplir la carga de argumentación que pesa sobre la parte recurrente*".

Tampoco podrá apreciar el TC la vulneración del derecho a la libertad de información (20.1.d CE), derecho que claramente es el que se pone en juego cuando se trata de despidos de *whistleblowers*, tal y como se ha expuesto más arriba (y como argumentaron, por ejemplo, la STC 6/1988, de 21 de enero de 1988 antes citada —ECLI:ES:TC:1988:6— o la STC 126/2003, de 30 de junio —ECLI: ES: TC: 2003:126—, o el propio fundamento jurídico cuarto de la sentencia 146/2019), pues los *whistleblowers*, en realidad, comunican "*información que se refiere a la difusión de hechos que merecen ser considerados noticiables*" (comunicación que debe cumplir, además, el canon de constitucionalidad que requiere expectativa de veracidad —fundamento 3 de la STC 126/2003, de 30 de junio—, obtención de la información con diligencia y afectación al interés público de esa información). Es decir, la actuación del *whistleblower* no se limita "*a expresar pensamientos, ideas y opiniones*" (objeto de la libertad de expresión del artículo 20.1.a CE), sino que consiste en informar, de ahí que sea más preciso concluir que el derecho en juego es el 20.d) CE, pues en realidad el hecho de transmitir esa información en forma de denuncia es el "interés preponderante" de los *whistleblowers*.

El TC se encuentra en este caso, no obstante, con el problema de que "*no se puede conocer si se facilitaron datos que sean constatables, y que no hay forma de poder determinar la veracidad o no en los mismos*" (tal y como apunta el fiscal en el antecedente octavo de la sentencia 146/2019). En realidad se trata de un problema que la jurisprudencia constitucional ya ha resuelto (no se requiere una veracidad absoluta, como recuerda la STC 6/1988) y que quizá quede más claro, si cabe, en la ley de transposición en el futuro, dado que la Directiva prevé que los denunciantes tienen derecho a la protección cuando tengan "*motivos razonables para pensar que la información sobre infracciones denunciadas es veraz en el momento de la denuncia*" (artículo 6.1.a de la Directiva), sin que se les requiera una verdad objetiva.

En todo caso, en la sentencia 146/2019 lo relevante es que el TC no tiene forma de determinar esa veracidad (y, entendemos, esa expectativa de veracidad). Ante esta dificultad, el TC deja de lado la libertad de información y pasa a analizar si se vulneró el derecho a la libertad de expresión, pues "*fueron las opiniones y juicios de valor del recurrente en amparo, y no el juico sobre la veracidad y el carácter noticiable de los hechos en los que se pudieron apoyar, el fundamento de la decisión extintiva*" y "*tanto la carta de advertencia como el posterior despido vincularon la decisión extintiva a los juicios de valor y quejas formuladas por el trabajador*".

Así, el TC estima el recurso de amparo considerando que el ejercicio del derecho a la libertad de expresión por parte del *whistleblower* se ejercitó de manera correcta (sin uso de expresiones ultrajantes —nunca la empresa le reprocha un tono duro en la forma de la comunicación—) y aprecia que la empresa adjudicataria empleadora prestaba servicios de tipo social (por tanto, tiene en cuenta el interés público y las circunstancias en las que se produ-

35 Eduardo Rojo Torrecilla: "La protección del derecho constitucional a la libertad de expresión en el ámbito de las relaciones de trabajo. Notas a la sentencia del TC núm. 146/2019, de 25 de noviembre". Disponible en http://www.eduardorojotorrecilla.es/2019/12/la-proteccion-del-derecho.html.

ce la crítica). El profesor Rojo Torrecilla[36] ha expuesto en relación con esta sentencia que "*a mi parecer, y más que aquello que se afirma en la sentencia, creo que se trata de reforzar la protección constitucional de la libertad de expresión en un supuesto en el que está*[n] *en juego intereses públicos y no solamente vinculados estrictamente a unas relaciones contractuales*".

b) Escaso y disperso derecho positivo

En el plano del derecho positivo, el artículo 48 de la Ley Orgánica 3/2007, de 22 de marzo de 2007, de Igualdad[37] ("Ley de Igualdad"), fue pionero en el ámbito laboral en el establecimiento de canales de denuncias, en concreto en el marco del acoso sexual y por razón de sexo. Su apartado primero estableció que "[...] *las empresas deberán* [...] *arbitrar procedimientos específicos para su prevención* [del acoso sexual y por razón de sexo] *y para dar cauce a las denuncias o reclamaciones que puedan formular quienes hayan sido objeto del mismo*". Además, indicó que se podrán establecer medidas que deberán negociarse con los representantes de los trabajadores, tales como la elaboración y difusión de códigos de buena prácticas, la realización de campañas informativas o acciones de formación.

La Ley de Igualdad propició la modificación de algunos artículos del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social[38] ("LISOS"). Así, se prevé como infracción muy grave en materia de relaciones laborales la represalia al *whistleblower*, a la que se refiere como "[...] *las decisiones del empresario que supongan un trato desfavorable de los trabajadores como reacción ante una reclamación efectuada en la empresa* [...] *destinada a exigir el cumplimiento del principio de igualdad de trato y no discriminación*" (artículo 8.12 de la LISOS). También se sanciona la omisión del empresario ante las denuncias recibidas en relación con el acoso de cualquier tipo cuando "[...] *conocido por el* [empresario], éste no hubiera adoptado las medidas necesarias para *impedirlo*" (artículo 8.13 bis de la LISOS). Las sanciones pueden oscilar entre 6251 euros y 187.515 euros (artículo 40.1.c de la LISOS) y, adicionalmente, se impondrán sanciones accesorias, puesto que (i) "*perderán automáticamente, y de forma proporcional al número de trabajadores afectados por la infracción, las ayudas, bonificaciones y, en general, los beneficios derivados de la aplicación de los programas de empleo*"; y (ii) "*podrán ser excluidos del acceso a tales beneficios por un período de 6 meses a dos años*" (artículo 46 bis de la LISOS).

Por último, y ya en el ámbito del despido, los *whistleblowers* cuentan en efecto con una protección genérica, pero amplia en su aplicación. Si su despido obedece a una discriminación o se ha producido mediante la vulneración de sus derechos fundamentales (por ejemplo, en caso de represalia por vulneración del derecho a la tutela judicial efectiva en su vertiente de protección a la garantía de indemnidad[39], o bien en caso de vulneración de su derecho a la libertad de información, o de expresión[40] o, incluso, si como apunta Lousada Arochena[41] se considera que se ha vulnerado el derecho a la protección de datos del *whistleblower* en caso de que "*se haya producido un acoso o represalia consiguiente a la denuncia porque* [...] *se ha vulnerado la confidencialidad en la gestión de los datos personales* [en el canal de denuncias]"), como hemos visto, será nulo —artículo 55.5 del Estatuto de los Trabajadores ("ET") en relación con los artículos 24 y 20.1.a) de la Constitución española—. Las consecuencias de esa nulidad serían la readmisión del trabajador y el abono de los salarios devengados desde la fecha del despido hasta la fecha de la readmisión. Adicionalmente, en la medida en que se haya producido esa vulneración de derechos fundamentales del *whistleblower*, existiría la necesidad de

36 Eduardo Rojo Torrecilla: "La protección del derecho constitucional...", *op. cit.*

37 Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.

38 Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

39 En este sentido, conviene señalar la Sentencia del Tribunal Superior de Justicia de Andalucía, Sala de lo Social (sede de Sevilla), núm. 2911, de 2 de octubre de 2007 (ROJ: STSJ AND 11523/2007), que declara la nulidad del despido de un trabajador que entregó al director de personal de la empresa unas fotografías comprometedoras y fue despedido. Del mismo modo, la Sentencia del Tribunal Superior de Justicia del País Vasco, Sala de lo Social, núm. 1879, de 12 de julio de 2005 (ROJ: STSJ PV 3244/2005), trata el caso de un trabajador despedido por comunicar al servicio de intervención de la empresa varias irregularidades en la gestión y funcionamiento de su centro de trabajo. La empresa no pudo demostrar que el despido obedeciera a una causa distinta a la represión de la denuncia del actor y, en consecuencia, la Sala declaró su nulidad.

40 Además de la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Andalucía (Sevilla), Sección Primera, de 13 de diciembre de 2018 (N.º recurso 4378/2017), antes citada, conviene tener en cuenta la Sentencia del Tribunal Superior de Justicia del País Vasco, Sala de lo Social, núm. 1879, de 12 de julio de 2005 (ROJ: STSJ PV 3244/2005).

41 José Fernando Lousada Arochena: "Sistemas de denuncias internas (Whistleblowing) y derechos fundamentales en el trabajo", *Trabajo y Derecho*, n.º 52, abril de 2019.

reparar esa vulneración de derechos. Y es que toda vulneración de derechos conlleva un derecho a indemnización de acuerdo con el artículo 183.1 de la Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social, y con la doctrina de la Sala de lo Social del Tribunal Supremo (por todas, en su sentencia de 5 de octubre de 2017). Por tanto, cabría solicitar una indemnización adicional por daños morales en conexión con la vulneración de ese derecho fundamental, sin perjuicio de la compleja valoración de esos daños, cuestión en la que no podemos entrar aquí.

2.1.2 · Impacto de la Directiva

a) Ámbito de aplicación subjetivo (expansivo) de la Directiva

Destaca la expansión del concepto de trabajador que utiliza la Directiva al definir su ámbito de aplicación personal (artículo 3 de la Directiva), ya que no se limita al concepto de trabajador por cuenta ajena del artículo 1 del ET.

En su lugar, la Directiva se proyecta sobre toda la información obtenida en el "*contexto laboral*", considerando el contrato de trabajo en sentido amplio (artículo 4 de la Directiva).

Esta expansión es querida y buscada por la Directiva, que se centra en proteger a aquellos que "*están mucho más cerca de la fuente de información sobre posibles prácticas abusivas*"[42]. En este sentido, la Directiva argumenta que "*la protección debe extenderse también a otras categorías de personas físicas que, sin ser «trabajadores» en el sentido del artículo 45, apartado 1, del TFUE, puedan desempeñar un papel clave a la hora de denunciar infracciones del Derecho de la Unión y que puedan encontrarse en situación de vulnerabilidad económica en el contexto de sus actividades laborales*" (considerando 39 de la Directiva). En la misma línea, el considerando 37 señala que "*debe otorgarse protección a la gama más amplia posible de categorías de personas que* [...] *en virtud de sus actividades laborales, con independencia de su naturaleza y de si son retribuidas, disponen de un acceso privilegiado a información sobre infracciones que redundaría en interés de los ciudadanos denunciar y que pueden sufrir represalias si así lo hacen*".

Así, el ámbito de aplicación personal de la Directiva cubre, en concreto, no solo la amplísima noción de trabajador prevista en el artículo 45 del Tratado de Funcionamiento de la Unión Europea ("TFUE"), que incluye a los "*funcionarios*", sino también a los trabajadores no asalariados en el sentido del artículo 49 del TFUE, a las relaciones mercantiles (se cita, por ejemplo a los accionistas y personas pertenecientes al órgano de administración de una empresa, incluidos los miembros no ejecutivos), a los voluntarios y trabajadores en prácticas (independientemente de si perciben remuneración o no), así como a "*cualquier persona que trabaje bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores*".

Igualmente, el ámbito de aplicación personal abarca las relaciones laborales ya extinguidas y finalizadas (*alumni*), pero también comprende a aquellos informantes cuya relación laboral no se ha iniciado todavía al encontrarse en procesos de selección o de negociación precontractual. Se cierra, finalmente, el concepto de denunciante objeto de protección incluyendo a facilitadores, compañeros de trabajo o familiares del denunciante y a entidades jurídicas que sean propiedad del denunciante, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral.

En definitiva, como han señalado algunos autores: la "*buscada amplitud del alcance personal instituido en la Directiva* [...] *permite entrever la perspectiva de una aplicación de su contenido prácticamente indiscriminada y sin apenas excepciones, en consonancia con una perspectiva maximalista de lo que debe corresponder a la protección de tales situaciones*" (López Baelo[43]).

b) La obligación de implementación de canales de denuncia y de su gestión

Desde el punto de vista laboral, dos son, esencialmente, las obligaciones que viene a imponer la Directiva: (i) la implementación de canales de denuncia interna (artículo 8 de la Directiva); y (ii) la obligación de gestionar y realizar seguimientos de esos canales de denuncia interna (artículos 9 y 16 a 18 de la Directiva).

(i) La obligación de implantar los canales de denuncia interna resultará aplicable a las enti-

42 Considerando 39 de la Directiva, que alude a los "*proveedores*".

43 Raúl López Baelo: "*Whistleblowing* y relaciones laborales: informantes, garantías y mecanismos de denuncia", artículo ganador del premio de jóvenes laboralistas FORELAB 2019. Disponible en https://www.andersentaxlegal.es/recursos/doc/portal/2019/01/09/directiva-del-parlamento-europeo-y-del-consejo.pdf.

dades jurídicas del sector privado que tengan 50 o más trabajadores, o bien que, independientemente del número de trabajadores a los que empleen, entren en el ámbito de aplicación del Derecho de la Unión en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales y financiación del terrorismo, seguridad del transporte o protección del medio ambiente. Habrá que estar, por otra parte, a las leyes de transposición de la Directiva para comprobar si España decide exigir que las entidades del sector privado de menos de 50 trabajadores que realicen determinadas actividades puedan resultar incluidas (posibilidad que deja abierta el artículo 8.7 de la Directiva). Igualmente, la obligación de implantar los canales pesará sobre las entidades del sector público. De nuevo, España podrá decidir si exime de esta obligación a las entidades del sector público con menos de 50 trabajadores y a los municipios de menos de 10.000 habitantes (artículo 8.9 de la Directiva).

(ii) Por lo que respecta a la obligación de gestionar el canal de denuncias, la Directiva prevé que puedan "*gestionarse internamente por una persona o departamento designados al efecto o podrán ser proporcionados directamente por un tercero*" (artículo 8.5 de la Directiva). El considerando 3 de la Directiva declara que los canales de denuncia deben ser "*efectivos, confidenciales y seguros y garantizando la protección efectiva de los denunciantes frente a represalias*". El artículo 9 detalla esos principios inspiradores de las características que todo canal debe tener. En concreto, su diseño, establecimiento y gestión deben ser seguros y garantizar la confidencialidad tanto del denunciante como de cualquier tercero mencionado en la denuncia (artículo 9.1.a). Además, debe asegurarse que no accede a la denuncia personal no autorizado. La celeridad y la diligencia son otros dos rasgos que deben definir el funcionamiento del canal. Así, se debe acusar recibo de la denuncia en el plazo de siete días. Se debe designar a una persona o departamento imparcial que sea competente para seguir las denuncias de manera "diligente", denuncias que pueden ser anónimas (artículo 9.e), lo que cierra un debate ya superado en España desde la entrada en vigor del artículo 24.1 de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD") y que supera definitivamente anteriores posturas de la APD que no encajaban con la opinión del Grupo del Artículo 29. Además, se deberá ofrecer una respuesta en un "*plazo razonable que no será superior a tres meses a partir del acuse de recibo*" (artículo 9.1.f). Algún sector de la doctrina (Blázquez Agudo)[44] ha señalado como "*buena práctica*" la adopción de "*medidas cautelares, cuando sea preciso, mientras dure el proceso de investigación*". En la práctica, por ejemplo, separar al *whistleblower* físicamente del supuesto acosador, en temas de *mobbing*, o bien, cuando el convenio colectivo lo permita, llevar a cabo una suspensión de empleo y sueldo del infractor para facilitar el proceso de investigación (supuesto que prevé, por ejemplo, el convenio colectivo sectorial estatal de agencias de viajes).

La información sobre los procedimientos debe ser "clara y fácilmente accesible" (artículo 9.g de la Directiva). No en vano, debe recordarse también que "*empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información*" (artículo 24.1 LOPDGDD, *in fine*). Por otra parte, se prevé una libertad de forma en las vías de recepción de las denuncias: "*los canales deberán permitir denunciar por escrito o verbalmente, o de ambos modos. La denuncia verbal será posible por vía telefónica, o a través de otros sistemas de mensajería de voz y, previa solicitud del denunciante, por medio de una reunión presencial dentro de un plazo razonable*" (artículo 9.2 de la Directiva). En la gestión de estos canales deberá tenerse especial cuidado con el deber de confidencialidad respecto de la identidad del denunciante, que no deberá "*revelarse sin su consentimiento expreso*", así como con el "*derecho a la protección de datos*".

c) El estatuto de protección del denunciante

Junto con la obligación de implementación y gestión de canales de denuncia, la otra gran novedad que la Directiva introduce desde el prisma laboral es el estatus de protección del denunciante.

(i) *Requisitos para poder ampararse en el estatus de protección del denunciante: uso previo de los canales internos y expectativa de veracidad de la información que se revela*

44 Eva María Blázquez Agudo: "Canal de denuncias o Whistleblowing en el ámbito laboral", en Ana de la Puebla Pinilla y Jesús Mercader Uguina (dirs.): *Tiempo de reformas. En busca de la competitividad empresarial y de la cohesión social*, Valencia: Tirant lo Blanch, 2019, pág. 571.

El estatuto de protección del denunciante que introduce la Directiva requiere dos presupuestos de hecho para su aplicación (artículo 6.1 de la Directiva): (a) que el *whistleblower* "*haya denunciado por canales internos conforme al artículo 7 o por canales externos conforme al artículo 10, o hayan hecho una revelación pública conforme al artículo 15* [de la Directiva]"; y (b) que el *whistleblower* "[...] *tenga motivos razonables para pensar que la información sobre infracciones denunciadas es veraz en el momento de la denuncia y que la citada información entra dentro del ámbito de aplicación de la Directiva*" (es decir, que la revelación se refiere a las materias cubiertas en su ámbito de aplicación material —artículo 2 de la Directiva—).

Respecto a la primera cuestión, las formas importan y la norma lo recalca. La revelación no puede realizarse de cualquier manera —como ya muestran los ejemplos jurisprudenciales citados en el apartado 2.1.1(A)—. Ya apuntaba Del Rey Guanter[45] al analizar la normativa americana en esta materia a finales de los años ochenta (en concreto, el Estatuto de Wisconsin o el de Pennsylvania) que "*las normas que regulan el «whistleblowing» cumplen un objetivo adicional, que es el de establecer un cauce interno formal a la labor de denuncia por parte del empleado* [...] *con anterioridad a la «exteriorización» a la opinión pública. No es que esta última posibilidad* —«going public»— *se prohíba, sino que se desincentiva como vía inicial mediante la aplicación de la protección estatutaria exclusivamente a los empleados que hayan utilizado el procedimiento interno legalmente establecido*".

La idea de seguir los cauces establecidos y de que la revelación directa a los medios sea la última medida a tomar ya la apuntó el TEDH[46] en el año 2008, al razonar que "*la divulgación al público no debe considerarse más que como último recurso, en caso de imposibilidad manifiesta de actuar de otro modo*", y fue tenida en cuenta en la elaboración de la Propuesta de Directiva, como señalaba su considerando 57.

De hecho, el artículo 7.2 de la Directiva refuerza esta cuestión al prever que "*los Estados miembros promoverán la comunicación a través de canales de denuncia interna antes que la comunicación a través de canales de denuncia externa, siempre que se pueda tratar la infracción internamente de manera efectiva y siempre que el denunciante considere que no hay riesgo de represalias*", y en términos similares recalca esa prioridad de uso de los canales internos en los artículos 10 y 15.1.a).

De hecho, para que el *whistleblower* cuente con el estatuto de protección en caso de revelación pública, se exige que haya denunciado primero por canales internos y externos, o directamente por los canales externos de conformidad con los capítulos II y III [de la Directiva] sin que se hayan tomado medidas apropiadas o bien que (a) tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público, como, por ejemplo, cuando se da una situación de emergencia o existe un riesgo de daños irreversibles, o (b) si realiza una denuncia externa del artículo 10 de la Directiva, "existe un riesgo de represalias o hay pocas probabilidades de que se dé un tratamiento efectivo a la infracción debido a las circunstancias particulares del caso" (ocultación de pruebas o connivencia de las autoridades con el autor de la infracción).

Por tanto, para gozar del estatuto de protección, conviene asegurarse de que se cumplen los requisitos de que se priorice el uso del canal de denuncia interna, posteriormente la denuncia externa y, finalmente, la revelación pública.

El análisis sobre la prelación del uso de medios internos, antes de acudir a medios externos o a la revelación pública, se puede observar, no obstante, en las sentencias de las que disponemos antes de la publicación y transposición de la Directiva. Buena muestra de ello puede apreciarse en la STC 146/2019 antes comentada —apartado 2.1.1(A)—, que aborda este debate, esto es, la necesidad de emplear en primer lugar los canales internos de la empresa para formular las denuncias (formulación de denuncias internas), antes de comunicarlas por canales externos o realizar revelaciones públicas (artículo 6.1 de la Directiva), que es el criterio inspirador de la Directiva que siempre se ha seguido —por ejemplo, entre otras, en la Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala, caso Guja contra

45 Salvador del Rey Guanter: *Libertad de expresión e información..., op. cit.,* pág. 101.

46 Tribunal Europeo de Derechos Humanos, Gran Sala, caso Guja contra Moldavia, demanda núm. 14277/04, de 12 de febrero de 2008 (ECLI:CE:ECHR:2008:0212JUD001427704).

Moldavia, de 12 de febrero de 2008 (ECLI: CE: ECHR: 2008: 0212JUD001427704)[47]—.

La STC 146/2019, a diferencia de lo resuelto en suplicación en ese procedimiento, entiende que el *whistleblower* formuló la denuncia correctamente, porque "*formuló sus quejas, en primer lugar, y ante todo, frente a su propia empleadora* [...] *y que solo una vez desatendidas sus reivindicaciones las fromul*[ó]*, en segundo lugar, ante el propio ayuntamiento*". Por tanto, realiza el análisis de si se priorizó la formalización de la denuncia por los canales internos, encontrando respuesta afirmativa a la cuestión. Y otorgó el amparo al *whistleblower* por vulneración de su derecho a la libertad de información.

Como contrapunto a la STC 146/2019, la STC 126/2003, de 30 de junio denegó el amparo al *whistleblower,* quien, en este último supuesto, acudió a la radio y a la prensa (diario *El Correo* y revista *Interviú*) para informar de graves irregularidades en una empresa de explosivos en Galdácano que "*en caso de explosión podría afectar de una manera importante*" a esta población. Los titulares de la época señalaban: "Esta empresa es una bomba".

En este último supuesto, el TC denegó el amparo a la vulneración del derecho a la información que se solicitaba. Y uno de los argumentos fundamentales para tal denegación fue el hecho de que el *whistleblower* aquí no esperó a recibir *feedback* de la empresa en cuanto a la denuncia interna y que, además, no era "*necesario que las informaciones difundidas alcanzasen la reiteración, la trascendencia y la notoriedad públicas que obtuvieron, ni dada su gravedad, debía considerase medio adecuado para su conocimiento la publicación en medios de comunicación de difusión nacional y local* [...], [lo que provocó] *una clara afectación de los intereses empresariales*" con notable menoscabo de su imagen pública.

Por tanto, como puede verse, la prelación del uso de los canales internos ya viene resultando capital en los supuestos resueltos por el TC.

Respecto de la segunda cuestión, la expectativa de veracidad del denunciante, el considerando 32 de la Directiva se encarga de aclarar que "[...] [p]*ara gozar de protección* [...]*, los denunciantes deben tener motivos razonables para creer, a la luz de las circunstancias y de la información de que dispongan en el momento de la denuncia, que los hechos que denuncian son ciertos. Ese requisito es una salvaguardia esencial frente a denuncias malintencionadas, frívolas o abusivas, para garantizar que quienes, en el momento de denunciar, comuniquen deliberada y conscientemente información incorrecta o engañosa no gocen de protección. Al mismo tiempo, el requisito garantiza que la protección no se pierda cuando el denunciante comunique información inexacta sobre infracciones por error cometido de buena fe. De manera similar, los denunciantes deben tener derecho a protección en virtud de la presente Directiva si tienen motivos razonables para creer que la información comunicada entra dentro de su ámbito de aplicación. Los motivos de los denunciantes al denunciar deben ser irrelevantes para determinar si esas personas deben recibir protección*".

La doctrina ha recalcado que "*lo que importa es que el denunciante crea en la veracidad de los hechos que va a poner en comunicación de la empresa, esto es, en que tenga buena fe, con independencia de que la información sea finalmente veraz o no*" (Nieto Rojas[48]). En términos similares se han pronunciado Blázquez Aguado[49] y la profesora Lozano Cutanda[50]. Esta última ha precisado que "*no se protege, por consiguiente, a quienes comuniquen deliberadamente información incorrecta o engañosa (que deberán ser sancionados por ello), pero sí a quienes comuniquen información inexacta sobre infracciones por error cometido de buena fe. Los motivos para denunciar se consideran irrelevantes a efectos de aplicar la protección de la directiva*".

En este punto, debemos recordar que no se exige una veracidad absoluta, pues su "*total exactitud puede ser controvertible*", sino que lo que se exige es un deber de diligencia del informador, a quien se le puede y debe exigir que lo que transmita como «hechos» haya sido objeto de previo contraste con datos objetivos, privándose, así, de la garantía constitucional a quien, defraudando el derecho de todos a la información, actúe con menosprecio de la verdad o falsedad de lo comunicado —fundamento de derecho quinto de la STC 6/1998—.

47 https://hudoc.echr.coe.int/spa#("itemid":["001-139375"])

48 Patricia Nieto Rojas: "Whistleblowers. Aspectos laborales de la Directiva...", *op. cit.*

49 Eva María Blázquez Agudo: "Canal de denuncias o *Whistleblowing* en el ámbito laboral", *op. cit.,* pág. 578.

50 Blanca Lozano Cutanda: "La directiva de protección del denunciante", *Diario La Ley*, n.º 9550, Sección Tribuna, 10 de enero de 2020.

(ii) *Afectación a las cláusulas contractuales de confidencialidad y propiedad de la empresa*

La Directiva pretende tutelar a los informantes, también en el ámbito de las responsabilidades que pueden afrontar como consecuencia de esa revelación de información (por ejemplo, en caso de que, al revelarla, el informante haya vulnerado las cláusulas de confidencialidad o de devolución de elementos propiedad de la empresa pactadas en el contrato de trabajo).

La Directiva razona, en sus considerandos 91 y 92, la necesidad de otorgar esa seguridad al informante y de ponerle a resguardo del incumplimiento de los acuerdos de confidencialidad y cláusulas de propiedad de la empresa, y explicita que "*no debe ser posible ampararse* [en ellas] [...] *para impedir las denuncias, para denegar la protección o para penalizar a los denunciantes por haber comunicado información sobre infracciones o haber efectuado una revelación pública cuando facilitar la información que entre dentro del alcance de dichas cláusulas y acuerdos sea necesario para revelar la infracción. Cuando se cumplan esas condiciones, los denunciantes no debe incurrir en responsabilidad alguna ya sea civil, penal, administrativa o laboral*". En definitiva, la Directiva pretende, de manera clara, que los informantes "*gocen de inmunidad frente a dicha responsabilidad*".

Por ello, el legislador, consciente de que los informantes, al revelar información, pueden verse expuestos a esas responsabilidades, ha querido garantizarles que "*no incurrirán en responsabilidad de ningún tipo como consecuencia de denuncias o de revelaciones públicas en virtud de la presente Directiva*" y que "*tendrán Derecho a alegar en su descargo el haber denunciado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la denuncia o revelación pública era necesaria para poner de manifiesto una infracción en virtud de la presente Directiva*" (artículo 21.7 de la Directiva y, en términos similares, artículo 21.2 de la Directiva). La protección no comprende, sin embargo, la "*información superflua*" revelada a no ser que existan "*motivos fundados*". Esta protección a los informantes se extiende específicamente a las "*solicitudes de indemnización basadas en el Derecho laboral privado*".

De obligada cita en este punto es el artículo 2.3 de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (la "Ley 1/2019"), mediante la que se traspone al ordenamiento español la Directiva 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, a fin de armonizar la legislación de los Estados miembros con el objetivo de establecer un nivel suficiente y comparable de reparación en todo el mercado interior en caso de apropiación indebida de secretos empresariales. Y ello porque establece que "*no procederán las acciones y medidas previstas en esta ley*" cuando "*se dirijan contra actos de obtención, utilización o revelación de un secreto empresarial que haya tenido lugar en cualquiera de las circunstancias siguientes*": (i) en el ejercicio del derecho a la libertad de expresión e información recogido en la Carta de los Derechos Fundamentales de la Unión Europea; (ii) con la finalidad de descubrir, en defensa del interés general, alguna falta, irregularidad o actividad ilegal que guarde relación directa con el secreto empresarial; (iii) al ponerlo en conocimiento de sus representantes para el ejercicio legítimo de las funciones que tienen legalmente atribuidas; y (iv) al tratar de proteger un interés legítimo reconocido por el Derecho europeo o español.

La doctrina (De la Puebla Pinilla[51]) ha interpretado aquí que "(...) *esta previsión podría alcanzar a aquellas informaciones sobre las que aun siendo secretas, los trabajadores tienen interés o deber ético de poner en conocimiento de sus representantes*" y que el artículo 2.2. podría estar remitiendo "*siquiera implícitamente, a los denominados canales de denuncia interna, los denominados whistleblowing*". En todo caso, la interacción entre la excepción del artículo 2.3 de la Ley 1/2019 y la Directiva es un punto complejo y delicado que habrá que seguir con detenimiento y sobre el que quizá la ley de transposición de la Directiva pueda realizar alguna aclaración.

De interés resulta, igualmente, el artículo 2.3.c) de la Ley 1/2019 que alude a la puesta en conocimiento de la denuncia a los representantes de los trabajadores. En este punto, y aunque los canales de denuncia internos tienen como habitual receptor a la empresa, conviene apuntar que "*nada impide que se prevea la creación de un*

51 Ana de la Puebla Pinilla: "Impacto laboral de la ley de secretos empresariales", en Ana de la Puebla Pinilla y Jesús Mercader Uguina (dirs.): *Tiempo de reformas...*, op. cit., pág. 516.

comité de ética o similar integrado también por representantes de los trabajadores, en cuyo caso cobra sentido la referencia que el artículo 2.3.c) Ley 1/2019 hace a la licitud de la revelación de secretos empresariales por los trabajadores cuando lo pongan en conocimiento de sus representantes"[52]. En esta misma línea, el posible rol de los representantes de los trabajadores como destinatarios de las denuncias (esto es, su posible autorización como receptores de denuncias, como si fueran un canal interno) ha sido sugerido por Mercadé Piqueras[53], *legal officer* de la Dirección General de Justicia en la Comisión Europea.

(iii) *El nuevo concepto de "represalia" al denunciante*

En el capítulo sexto se encuentra el corazón de la Directiva, en el que cristalizan las medidas específicas de protección de los informantes.

Entre ellas, se instaura la prohibición de "*todas las formas de represalia*" (artículo 19 de la Directiva) y se desglosa el extenso catálogo de represalias, casi todas ellas con un contenido eminentemente laboral. La Directiva configura aquí un concepto muy extenso de represalia, que comprende las siguientes situaciones: (a) suspensión, despido, destitución o medidas equivalentes; (b) degradación o denegación de ascensos; (c) cambio de puesto de trabajo, cambio de ubicación del lugar de trabajo, reducción salarial o cambio del horario de trabajo; (d) denegación de formación; (e) evaluación o referencias negativas respecto a sus resultados laborales; (f) imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las pecuniarias; (g) coacciones, intimidaciones, acoso u ostracismo; (h) discriminación, o trato desfavorable o injusto; (i) no conversión de un contrato de trabajo temporal en indefinido; (j) no renovación o terminación anticipada de un contrato de trabajo temporal; (k) daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos; (l) inclusión en listas negras; (m) terminación anticipada o anulación de contratos de bienes o servicios; (n) anulación de una licencia o permiso; o, finalmente, (ñ) referencias médicas o psiquiátricas.

Conviene señalar, como se ha encargado de apuntar López Cumbre 54, que el listado del artículo 19 de la Directiva tiene carácter de *numerus apertus*, "*dado que la propia disposición alude a* «toda forma de represalia», *amparando así cualquier tipo de comportamiento empresarial que suponga un reproche al trabajador denunciante por su actuación*". Es cierto que el catálogo de represalias, "*aun cuando el ámbito de aplicación subjetivo excede de los rasgos propios del trabajador*", se centra en "*prohibiciones expresas* [que] *se circunscriben a la relación laboral*", aunque se prevén "*con menor precisión, otras de diferente naturaleza (pérdida del negocio, terminación anticipada o anulación del contrato de bienes o servicios, etc.)*". En todo caso, el listado es de utilidad para contar con una definición de represalia con múltiples ejemplos de la que se carecía hasta la fecha en la legislación laboral, por tanto, se trata de una buena oportunidad para el legislador en la elaboración de la norma de transposición de la Directiva en estos próximos dos años.

(iv) *Instrumentos de defensa procesal*

La Directiva va un paso más allá en la protección específica de los informantes en el proceso al incluir la inversión de la carga de la prueba y las medidas cautelares.

Respecto de la primera cuestión, el considerando 93 de la Directiva señala que "*una vez que el denunciante demuestre, razonablemente, que ha denunciado infracciones o que ha efectuado una revelación pública de conformidad con la presente Directiva y que ha sufrido un perjuicio, la carga de la prueba debe recaer en la persona que haya tomado la medida perjudicial, a quien se debe entonces exigir que demuestre que las medidas adoptadas no estaban vinculadas en modo alguno a la denuncia o la revelación pública*".

La Directiva concreta lo anterior en una protección en los procedimientos "*relativos a los perjuicios sufridos por los denunciantes*", en los que, cuando se haga constar que el informante ha "*denunciado o ha hecho una revelación pública y que ha sufrido un perjuicio, se presumirá que el*

52 Ana de la Puebla Pinilla: "Impacto laboral de la ley de secretos empresariales", *op. cit.*, pág. 516.

53 Christel Mercadé Piqueras: "El canal de denuncias internas (*Whistleblowing*): La perspectiva laboral, investigación, garantías y deber de protección de datos", ponencia impartida en el marco del XX Congreso de ASNALA. Segovia, 26 de octubre de 2019.

54 Lourdes López Cumbre: "Protección para los trabajadores denunciantes (*whistleblowers*)", *Análisis GA_P*, diciembre 2019. Disponible en https://www.ga-p.com/wp-content/uploads/2019/12/Protección-para-los-trabajadores-denunciantes-whistleblowers.-1.pdf

perjuicio se produjo como represalia por denunciar o hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados" (artículo 21.5 de la Directiva).

Respecto de la segunda cuestión, el considerando 96 de la Directiva contempla el derecho del informante a "*acogerse a medidas provisionales tal como se establezcan en Derecho nacional*". Su objetivo será "*poner fin a amenazas, tentativas o actos continuados de represalia, como el acoso, o para prevenir formas de represalia como el despido, que puede ser difícil de revertir una vez transcurrido un largo período y arruinar económicamente a una persona*". Este punto ha cristalizado en la Directiva al garantizar que los informantes cuenten con "*acceso a medidas correctoras frente a represalias* (...), *incluidas medidas provisionales a la espera de la resolución del proceso judicial*" (artículo 21.6 de la Directiva).

2.2 · La directiva desde la perspectiva del Derecho público

2.2.1 · Panorama previo a la publicación de la Directiva

Dentro del "cajón de sastre" que, desde cierto punto de vista, constituye el Derecho público (en su acepción más amplia), el panorama existente en nuestro ordenamiento jurídico, antes de la publicación de la Directiva, en materia de protección de los "denunciantes" o *whistleblowers*, es ciertamente heterogéneo. Si bien no existe una disposición normativa que se haya ocupado de regular, desde un punto de vista integral, la figura del denunciante y su estatuto jurídico (al menos no en los términos a los que va a obligar la transposición de la Directiva)[55], determinada legislación sectorial sí se ha ocupado, cuando menos, de establecer determinadas previsiones sobre *whistlebowing* y protección jurídica de los *whistleblowers*, bien por propia iniciativa del legislador español, bien por la necesidad de transponer a nuestro ordenamiento jurídico otras disposiciones del Derecho de la Unión Europea en las que ya se contemplaban medidas de esta naturaleza.

Un análisis pormenorizado y exhaustivo de la legislación estatal[56] que puede recoger, en mayor o menor medida, previsiones sobre la figura del denunciante y su protección jurídica y laboral, y que habilita, también en mayor o menor medida, medios o canales para hacer llegar esa denuncia a las autoridades públicas competentes, excedería, con mucho, el objeto de este trabajo. No obstante, es posible apuntar, de forma necesariamente sintética, algunas disposiciones normativas que evidencian el heterogéneo sustrato normativo en el que viene a incidir ahora la Directiva[57].

a) La figura de la "denuncia" y del "denunciante" en la legislación del procedimiento administrativo común de las Administraciones públicas

La figura de la "denuncia" (e, implícitamente, la del propio "denunciante"), como "*acto por el que una persona, en cumplimiento o no de una obligación legal, pone en conocimiento de un órgano administrativo la existencia de un determinado hecho que pudiera justificar la iniciación de oficio de un procedimiento administrativo*", se recoge, en nuestro ordenamiento jurídico-público, en el apartado primero del artículo 62 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas ("LPAC")[58].

55 En septiembre de 2016, se llegó a presentar para su tramitación por el Congreso de los Diputados una Proposición de Ley Integral de Lucha contra la Corrupción y Protección de los Denunciantes, que hubiera supuesto un verdadero hito normativo en esta materia, con anterioridad, incluso, a la aprobación y publicación de la Directiva. No obstante, los avatares sobradamente conocidos de las últimas legislaturas paralizaron *sine die* su tramitación parlamentaria. A este respecto, *vid*. M.ª Concepción Campos Acuña: "Modificación de la Ley de Transparencia en la Propuesta de Ley de Lucha Integral contra la corrupción y protección de los denunciantes", *El Consultor de los Ayuntamientos*, n.º 2, 2018.

56 El análisis que sigue a continuación se va a circunscribir a la legislación estatal, dejando a un lado posibles previsiones normativas que hayan podido aprobar, en esta materia, las Comunidades Autónomas. Existen, no obstante, ejemplos autonómicos de medidas legislativas de protección de los denunciantes. Así, las Cortes de Castilla y León aprobaron, ya en el año 2016, la Ley 2/2016, de 11 de noviembre, por la que se regulan las actuaciones para dar curso a las informaciones que reciba la Administración Autonómica sobre hechos relacionados con delitos contra la Administración Pública y se establecen las garantías de los informantes.

57 La transposición de la Directiva a nuestro ordenamiento jurídico, nos atrevemos a anticipar, deberá efectuarse, necesariamente, por medio de una norma con rango legal. Así se deduce, en nuestra opinión, de la propia naturaleza de las "*Medidas de protección*" que, de acuerdo con el capítulo VI de la Directiva, los Estados miembros deben implementar en sus respectivos ordenamientos jurídicos para darle efectivo cumplimiento.

58 Este precepto, titulado "*Inicio del procedimiento por denuncia*", se inserta en la sección 2.ª del capítulo II del título IV de la LPAC, en la que se regulan los distintos modos de "*Iniciación del procedimiento de oficio por la administración*", lo que da fe de su carácter marcadamente instrumental respecto de un subsecuente proceder administrativo, fundamentalmente de carácter

El artículo 62 de la vigente LPAC constituye un desarrollo normativo, sin duda notable, de la escueta mención a la "denuncia", como una de las razones o motivos que podían dar lugar a la iniciación de oficio de un procedimiento por parte de una Administración, que se recogía en el inciso final del artículo 69.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Este desarrollo normativo mantiene, no obstante, la tradicional vinculación de la denuncia (y de la figura del denunciante) con el posterior ejercicio del *ius puniendi* por parte de una Administración pública, de ahí que hayan sido la doctrina y la jurisprudencia en materia de Derecho administrativo sancionador las que se hayan ocupado, con mayor detenimiento, en analizar y delimitar tanto su naturaleza como sus contornos jurídicos[59].

El artículo 62.2 de la LPAC exige, en todo caso, que "*Las denuncias deberán expresar la identidad de la persona o personas que las presenten*", sin que, en franco contraste con lo dispuesto en el artículo 16 de la Directiva ("*Deber de confidencialidad*"), se articulen ni contemplen mecanismos concretos para velar o garantizar que no se revele la identidad del denunciante más que a miembros autorizados del personal que debe recibir o gestionar las denuncias. Se trata, pues, de una de las cuestiones en las que la transposición de la Directiva deberá incidir, para adecuar nuestro ordenamiento jurídico a sus previsiones, eminentemente más protectoras y garantes para el denunciante, en este punto, que las que existen hoy en día en nuestro ordenamiento jurídico.

Si bien, en sentido estricto, es difícilmente catalogable como una medida de protección, merece una mención especial el singular (y ambicioso) incentivo que, para el denunciante, se contempla en el apartado cuarto del artículo 62 de la LPAC, sin parangón en el texto de la Directiva (aunque, a nuestro juicio, nada de lo que en ella se establece impediría que los Estados miembros pudieran articular una sistema de incentivos de esta naturaleza, aprovechando su necesaria transposición, en sus respectivos ordenamientos jurídicos[60]).

Así, a tenor del primer párrafo del artículo 62.4 de la LPAC[61]:

> "*Cuando el denunciante haya participado en la comisión de una infracción de esta naturaleza y existan otros infractores, el órgano competente para resolver el procedimiento deberá eximir al denunciante del pago de la multa que le correspondería u otro tipo de sanción de carácter no pecuniario, cuando sea el primero en aportar elementos de prueba que permitan iniciar el procedimiento o comprobar la infracción, siempre y cuando en el momento de aportarse aquellos no se disponga de elementos suficientes para ordenar la misma y se repare el perjuicio causado*"[62].

Como se puede comprobar, con la finalidad de incentivar tanto la denuncia de potenciales hechos constitutivos de una infracción administrativa en la que hayan concurrido diversos sujetos como la colaboración con las correspondientes autoridades en su investigación, el artículo 62.4 de la LPAC habilita expresamente al órgano de la Administración que resulte competente para resolver el procedimiento sancionador a que exima al infractor-denunciante del pago de la multa (o del cumplimiento de otra sanción cuando esta no sea de carácter pecuniario).

sancionador. No obstante, precisamente por su vinculación fundamental con el ejercicio de potestades sancionadoras por parte de las Administraciones públicas, en su regulación legal se contemplan algunas previsiones sustantivas sobre protección del denunciante, en determinadas circunstancias, que excederían, incluso, de las previstas en la Directiva, como se verá a continuación.

59 Así lo revela, a nuestro juicio con claridad, el hecho de que el artículo 62 de la LPAC señale, en su apartado segundo, que "*Cuando dichos hechos pudieran constituir una infracción administrativa,* [las denuncias] *recogerán la fecha de su comisión y, cuando sea posible, la identificación de los presuntos responsables*". Existe una abundante jurisprudencia sobre la naturaleza y delimitación de la "denuncia" como uno de los "modos" que pueden dar lugar a la iniciación de oficio de un procedimiento, en especial, de un procedimiento sancionador, por parte de una Administración. Pueden citarse, por todas, las Sentencias del Tribunal Supremo de 23 de junio de 1987 (referencia Aranzadi RJ 1987, 6524), de 3 de julio de 1990 (referencia Aranzadi RJ 1990, 8693) o de 11 de abril de 2006 (referencia Aranzadi RJ 2006, 2152).

60 De hecho, el artículo 25.1 de la Directiva dispone expresamente que "*Los Estados miembros podrán introducir o mantener disposiciones más favorables para los derechos de los denunciantes que los establecidos en esta Directiva* [...]", lo que refuerza nuestra anterior consideración.

61 La existencia de este incentivo, así como su carácter singular, en contraste con las previsiones de la propia Directiva, ha sido puesta de manifiesto, entre otros, por Javier Miranzo Díaz: "La nueva Directiva de protección del denunciante: un análisis desde el Derecho público", *Revista General de Derecho Europeo*, n.º 49, 2019.

62 Continúa señalando el precepto que "*Asimismo, el órgano competente para resolver deberá reducir el importe del pago de la multa que le correspondería o, en su caso, la sanción de carácter no pecuniario, cuando no cumpliéndose alguna de las condiciones anteriores, el denunciante facilite elementos de prueba que aporten un valor añadido significativo respecto de aquellos de los que se disponga*". Y finaliza señalando que "*En ambos casos será necesario que el denunciante cese en la participación de la infracción y no haya destruido elementos de prueba relacionados con el objeto de la denuncia*".

Esta exención, no obstante, se somete al cumplimiento de tres condiciones fundamentales: la primera, que el denunciante sea el primero en aportar "*elementos de prueba*" que posibiliten el inicio (fundado) del procedimiento sancionador o la comprobación de la infracción; la segunda, que en el momento en el que el denunciante aporte tales elementos de prueba, la Administración no dispusiera de otros elementos de prueba, obtenidos a través de otras fuentes, que le permitieran iniciar, en los mismos términos, el procedimiento sancionador; y, finalmente, que, en todo caso, repare el perjuicio que hubiera causado con la infracción (en el caso de que este fuera cuantificable o de posible determinación)[63].

El artículo 62.4 de la LPAC, en definitiva, ha pretendido generalizar, en el ámbito del Derecho administrativo sancionador, un mecanismo equivalente al de los *leniency programmes* ("programas de clemencia"), que gozan de una consolidada aplicación en diversas áreas jurídicas, sin ir más lejos, en la normativa de defensa de la competencia, tanto nacional como de la Unión Europea. No obstante, su efectiva aplicación es aún tímida por parte de las Administraciones públicas.

b) Las previsiones sobre *whistleblowing* recogidas en la legislación sectorial sobre entidades bancarias y servicios financieros

Como se ocupa de destacar de forma expresa el considerando 7 de la Directiva, "*En el ámbito de los servicios financieros, el valor añadido de la protección de los denunciantes ya ha sido reconocido por el legislador de la Unión*", y se citan específicamente, como actos de la Unión en los que se habían establecido ya distintas disposiciones sobre *whistleblowing* y protección de los *whistleblowers*, la Directiva 2013/36/UE[64] y el Reglamento (UE) 575/2013[65].

(i) La Ley 10/2014, de 26 de junio, de Ordenación, Supervisión y Solvencia de Entidades de Crédito ("LOSSEC"), recoge, dentro de su título III ("*Régimen sancionador*"), un capítulo V, sobre "*Comunicación de infracciones*" (arts. 119 a 122)[66].

El capítulo V del título III de la LOSSEC permite que "*Toda persona que disponga de conocimiento o sospecha fundada de incumplimiento de las obligaciones en materia de supervisión prudencial de entidades de crédito previstas en esta ley y su normativa de desarrollo, siempre que estén previstas en la Directiva 2013/36/UE, de 26 de junio, o en el Reglamento (UE) n.º 575/2013, de 26 de junio,* [pueda] *comunicarlo al Banco de España en la forma y con las garantías establecidas en este artículo*" (art. 119.1). Estas comunicaciones "*deberán presentarse por cualquier vía que permita la constancia fehaciente de la identidad del comunicante y de su presentación ante el Banco de España*" (art. 119.2), sin perjuicio de que el Banco de España articule "*medidas de protección de la identidad del comunicante*" (art. 119.3), en especial, garantías *ad hoc* de confidencialidad.

Por lo demás, la LOSSEC se ocupa de regular aspectos tales como el contenido mínimo de las comunicaciones (art. 120)[67], las garantías de confidencialidad "*del comunicante y de la información comunicada*" (art. 121) y, en fin, determinadas medidas de protección "*en el ámbito laboral y contractual*" (art. 122)[68]. Estas medidas pueden considerarse precedentes directos de las medidas de protección, más amplias y exhaustivas, dispensadas por la Directiva.

63 En nuestra opinión, atendiendo a una interpretación coherente de este precepto legal, así como a la práctica administrativa desarrollada por determinados órganos administrativos en materias en las que existe una mayor tradición en la aplicación de esta institución jurídica, tales como defensa de la competencia, el órgano administrativo debe resolver la concurrencia de tales condiciones, así como la efectiva aplicación de la sanción, en la resolución por la que se ponga fin al procedimiento administrativo sancionador.

64 Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE.

65 Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012.

66 Este capítulo V fue añadido al título III de la LOSSEC por la disposición final 6.10 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, y entró en vigor el 25 de noviembre de 2018.

67 Se prevé a este respecto que, "*Cuando la incoación del procedimiento sancionador se hubiese solicitado expresamente en la comunicación, el Banco de España informará a la persona que envía la comunicación del inicio, en su caso, de un procedimiento sancionador. Si tras la comunicación se iniciase procedimiento sancionador a partir de los hechos comunicados, el Banco de España informará de su inicio al comunicante. La comunicación no otorgará por sí misma la condición de interesado en el procedimiento sancionador a la persona comunicante*" (art. 120.3 de la LOSSEC).

68 Entre otras medidas de protección, se dispone expresamente que la comunicación de alguna de las infracciones previstas en el artículo 119 "*No constituirá infracción de ningún tipo en el ámbito de la normativa laboral por parte de la persona comunicante, ni de ella podrá derivar trato injusto o discriminatorio por parte del empleador*" (art. 122.1.b de la LOSSEC).

Por lo que se refiere, en concreto, a estas medidas de protección en el ámbito laboral y contractual, el artículo 122.1 de la LOSSEC contempla fundamentalmente tres medidas, de las que destaca especialmente la tercera por cuanto, *a priori*, parece plantear una importante salvedad (o contradicción) con el régimen diseñado en la Directiva. Así:

a) La primera de las medidas proporciona una exención a las posibles restricciones de divulgación de información "*impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa*" al denunciante ("*comunicante*" en terminología de la LOSSEC).

b) La segunda de las medidas exime de la consideración de infracción de la normativa laboral por parte del denunciante, apostillando que de ello no se podrá derivar ningún "*trato injusto o discriminatorio por parte del empleador*".

c) La tercera de las medidas —la que ofrece mayores dudas interpretativas en cuanto a su encaje con el régimen de la Directiva— excluye cualquier tipo de indemnización o compensación de la empresa en la que preste servicios el denunciante o de un tercero "*aun cuando se hubiera pactado la obligación de comunicación previa a dicha empresa o a un tercero*"[69].

(ii) Por su parte, siguiendo un esquema muy similar al incluido en la LOSSEC, el Texto Refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre ("TRLMV"), ha incorporado también un capítulo IV.bis, "*Comunicación de infracciones*", en su título VIII, relativo al "*Régimen de supervisión, inspección y sanción*" (arts. 276.bis a 276.sexies)[70].

Es de destacar que el artículo 276 del TRLMV, aunque ubicado inmediatamente antes del referido capítulo IV.bis, recoge un régimen de "*Condonación de infracciones*" propio específico, que, aunque tributario del contemplado en el artículo 62.4 de la LPAC, presenta características propias, puesto que habilita al Ministerio de Economía a, previo "informe de la CNMV, "*condonar, total o parcialmente, o aplazar el pago de las multas impuestas a personas jurídicas cuando hayan pasado a estar controladas por otros accionistas después de cometerse la infracción, estén incursas en un procedimiento concursal, o se den otras circunstancias excepcionales que hagan que el cumplimiento de la sanción en sus propios términos atente contra la equidad o perjudique a los intereses generales*".

También puede destacarse que, a diferencia de la LOSSEC, el art. 276.bis del TRLMV recoge una regulación más precisa y detallada de los "*Tipos y canales de comunicación de infracciones*". Las comunicaciones podrán realizarse (a) de forma escrita, en formato electrónico o papel, (b) de forma oral, por vía telefónica, que podría ser grabada, (c) a través de reunión física con el personal especializado de la CNMV; o (d) de cualquiera de las formas que establezca la persona titular del Ministerio de Economía y Empresa en norma reglamentaria adoptada a tal efecto.

Por lo demás, las medidas de protección en el ámbito laboral y contractual establecidas en el artículo 276.sexies del TRLMV son sustancialmente idénticas a las previstas en la LOSSEC, que se acaban de enunciar.

En cualquier caso, los canales de denuncia contemplados en la legislación sectorial sobre entidades bancarias y servicios financieros son, única y exclusivamente, canales de carácter externo a la propia entidad u organización en la medida en que solo están pensadas para permitir el flujo de información entre el denunciante (persona física) y el personal habilitado a tal efecto del Banco de España o de la CNMV. Desde este punto de vista, si bien las medidas de la LOSSEC y del TRLMV "anticipan" en buena medida la labor de transposición que habrá que hacer respecto de la Directiva, las medidas que en ellas se articulan resultan claramente insuficientes para dar debido cumplimiento a sus previsiones. En todo caso, no debería perderse la ocasión de tomarse en debida consideración la experiencia adquirida con su aplicación para los trabajos de

69 Las posibles dificultades de encaje con el régimen de la Directiva se derivarían de la prevalencia que se da en esta a las denuncias a través de canales de denuncia internos, esto es, dentro de la propia organización en la que presta servicios el denunciante. No obstante, es cierto que el artículo 122.1.c) de la LOSSEC solo hace referencia a los "pactos" entre las partes y no a una obligación normativa.

70 Este capítulo IV.bis fue añadido al título VIII del TRLMV por artículo único.75 del Real Decreto-ley 14/2018, de 28 de septiembre, por el que se modifica el texto refundido de la Ley del Mercado de Valores, aprobado por el Real Decreto Legislativo 4/2015, de 23 de octubre, y posteriormente modificado por la disposición final 9.21 del ya citado Real Decreto-ley 19/2018.

transposición para conseguir una mejor y más efectiva implementación de la Directiva.

c) Otra legislación sectorial con previsiones (parciales) en esta materia

Sin pretensión alguna de exhaustividad, otras normas que podríamos denominar sectoriales, aunque sea en un sentido lato, contemplan determinadas previsiones sobre *whistleblowing* y *whistleblowers*, si bien no con el carácter integral que inspira la Directiva.

Siguiendo en este punto a Bachmaier Winter[71], entre las normas legislativas españolas que recogen algún tipo de previsión sobre el establecimiento de canales de denuncia o protección de denunciantes se encontrarían, entre otras, las siguientes:

(i) La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, que, entre otras disposiciones, contempla el establecimiento de un canal de comunicación abierto e interactivo entre las Administraciones y los particulares, como el Portal de Transparencia.

(ii) La Ley 15/2007, de 3 de julio, de Defensa de la Competencia, en cuyo artículo 66 ("*Reducción del importe de la multa*") se regula el núcleo normativo de los denominados "programas de clemencia" (*leniency programmes*) para aquellos que colaboren, cumpliendo determinados requisitos, en la prevención y represión de las conductas contrarias a la competencia[72].

(iii) Finalmente, la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, que, a lo largo de su articulado, recoge ciertamente previsiones que ya anticipan, en este concreto ámbito material, las que la Directiva pretende extender, con carácter general o integral, a cualquier infracción del Derecho de la Unión Europea.

En definitiva, aunque con el alcance desigual y heterogéneo que se anticipaba al comienzo de este apartado, la legislación española no es desconocedora de las figuras de la "denuncia" y del "denunciante", así como de su protección. En esta realidad normativa es en la que "aterriza" (admítase la expresión) la Directiva.

d) Mención final a la normativa de contratación pública

Cabe hacer una breve mención, por último, a la normativa española de contratación pública, que es, precisamente, una de las materias que entran dentro del ámbito de aplicación de los actos de la Unión que, de acuerdo con lo previsto en su artículo 2.1, quedan amparados por aplicación de la Directiva[73].

De forma ciertamente sorprendente, pues a nadie se le escapa la relevancia de la contratación pública, tanto desde la perspectiva de la construcción del mercado interior como desde su perspectiva estrictamente económica, y a pesar de que fue (y ha sido) un tema efectivamente debatido, la vigente Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 ("LCSP"), no articuló finalmente (o, al menos, no directamente) canales de denuncia de posibles infracciones de contratación pública ni contempló medidas para la salvaguarda y protección de los denunciantes, entre otros aspectos.

No obstante, merece la pena señalar que el artículo 332 de la LCSP ha instituido la denominada Oficina Independiente de Regulación y Supervisión de

71 Lorena Bachmaier Winter: "*Whistleblowing* europeo y *compliance*: La Directiva EU de 2019 relativa a la protección de personas que reporten infracciones del Derecho de la Unión", *Diario La Ley*, n.º 9539, 18 de diciembre de 2019.

72 Las previsiones del artículo 66 de la Ley de Defensa de la Competencia se encuentran desarrolladas en la Sección 7.ª del capítulo II del título II (arts. 46 a 53) del Reglamento de Defensa de la Competencia, aprobado por Real Decreto 261/2008, de 22 de febrero.

73 El apartado A del Anexo I de la Directiva cita, entre las "*Normas de procedimiento aplicables a la contratación pública y la adjudicación de concesiones, a la adjudicación de contratos en los ámbitos de la defensa y la seguridad, y a la adjudicación de contratos por parte de entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y cualquier otro contrato*", las siguientes: (i) la Directiva 2014/23/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la adjudicación de contratos de concesión; (ii) la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE; (iii) la Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE (pendiente de transposición en España); y (iv) la Directiva 2009/81/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE.

la Contratación ("OIRSC"), órgano colegiado al que se encomienda "*velar por la correcta aplicación de la legislación y, en particular, promover la concurrencia y combatir las ilegalidades, en relación con la contratación pública*", y que disfruta de plena independencia orgánica y funcional (art. 332.1 LCSP). También cabe señalar que, en el desarrollo de sus funciones, la OIRSC se encuentra legalmente facultada para "*realizar encuestas e investigaciones, para lo que tendrá acceso a los órganos y servicios de contratación, que deberán facilitar los datos, documentos o antecedentes o cualquier información que aquella les reclame, salvo que tengan carácter secreto o reservado*" (art. 332.6, apartado b, de la LCSP).

Así pues, nada parece impedir (más bien al contrario) que, en lo que a la contratación pública se refiere, se habiliten canales de denuncia específicos para poner en conocimiento de la OIRSC potenciales infracciones e incumplimientos de la normativa en esta materia, proporcionándose a tal efecto protección singular tanto a aquellos denunciantes que trabajan en las Administraciones públicas y restantes entidades del sector público incluidos en su ámbito de aplicación (órganos de contratación) como en aquellas empresas y entidades que son contratistas públicos.

2.2.2 · Impacto de la Directiva

a) De la denuncia de una infracción administrativa a la denuncia de determinadas "infracciones" del Derecho de la Unión: el ámbito de aplicación material de la Directiva

De lo expuesto hasta ahora se deduce, con facilidad, que los distintos regímenes o sistemas existentes en la legislación española, desde luego en la de Derecho público, tienen como finalidad última (y esencial) poner en conocimiento de las Administraciones públicas la posible existencia de una infracción administrativa para, de esta manera, permitir o facilitar, en su caso, el ejercicio de sus potestades sancionadoras.

La Directiva, podría decirse, tiene una "filosofía" distinta, y es esta nueva "filosofía" la que debe ser trasladada a nuestro ordenamiento jurídico con su transposición. Su considerando 3 deja claro, en este sentido, que su ámbito de aplicación material viene determinado por "*las infracciones del Derecho de la Unión, con independencia de si el Derecho nacional las clasifica como administrativas, penales o de otro tipo*".

La calificación de la naturaleza de la infracción por el derecho nacional, por tanto, resulta irrelevante a los efectos de la Directiva (y, como es lógico, es una de las cuestiones que deberá tenerse en cuenta en su transposición). Lo relevante, de acuerdo con su artículo 2 ("Ámbito de aplicación material"), es la existencia, o la sospecha razonada y fundada de existencia, de "*infracciones del Derecho de la Unión*" que se encuentren referidas a una serie de ámbitos o áreas expresamente determinados en el citado precepto. Como ha puesto de manifiesto Miranzo Díaz, "*La Directiva exige* [...] *que la situación denunciada suponga —o haya fundamentos para creer de forma razonable que supone— una vulneración del Derecho de la UE, que puede tener lugar fruto de actos u omisiones. Al exigir que la denuncia se refiera a vulneraciones de derecho* [...] *el legislador europeo busca desincentivar el torpedeo malintencionado de las decisiones o las meras venganzas personales*"[74].

Pues bien, el artículo 2 de la Directiva establece las siguientes categorías de "*infracciones del Derecho de la Unión*" que quedan amparadas por el ámbito de aplicación material (u objetivo, por utilizar un término más común y propio de nuestro Derecho) de la Directiva:

(i) En primer lugar, aquellas "*infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo*" de la Directiva y que se encuentren referidas a las siguientes áreas o ámbitos jurídicos: (a) la contratación pública[75], (b) los servicios, productos y mercados financieros, la prevención del blanqueo de capitales y la financiación del terrorismo, (c) la seguridad de los productos y conformidad, (d) la seguridad del transporte, (e) la protección del medio ambiente, (f) la protección frente a las radiaciones y la seguridad nuclear, (g) la seguridad de los alimentos y los

74 Javier Miranzo Díaz: "La nueva Directiva de protección del denunciante...", *op. cit*.

75 Es importante hacer notar que, específicamente en materia de contratación pública, pero perfectamente generalizable al resto de las previsiones de la Directiva, la "*seguridad nacional*" queda expresamente excluida de su ámbito de aplicación al corresponder, en exclusiva, a los Estados miembros. Así, de acuerdo con lo indicado en el considerando 24: "*La seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. La presente Directiva no debe aplicarse a las denuncias de infracciones en materia de contratación pública que afecten a aspectos de la defensa o la seguridad cuando estos estén cubiertos por el artículo 346 del TFUE, de conformidad con la jurisprudencia del Tribunal de Justicia*". Sin perjuicio de ello, en ese mismo considerando se continúa señalando que "*Si los Estados miembros decidieran ampliar la protección que ofrece la presente Directiva a otros ámbitos o actos que no entren dentro de su ámbito de aplicación material, han de poder adoptar disposiciones específicas para proteger los intereses esenciales de su seguridad nacional a tal respecto*".

piensos, sanidad animal y bienestar de los animales, (h) la salud pública, (i) la protección de los consumidores, y (j) la protección de la privacidad y de los datos personales, y la seguridad de las redes y los sistemas de información (apartado 1.a del art. 2 de la Directiva).

(ii) En segundo lugar, aquellas "*infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE y tal como se concretan en las correspondientes medidas de la Unión*" (apartado 1.b del art. 2 de la Directiva)[76].

(iii) En tercer y último lugar, aquellas "*infracciones relativas al mercado interior, tal como se contemplan en el artículo 26, apartado 2, del TFUE, incluidas las infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades*" (apartado 1.c del art. 2 de la Directiva)[77].

En definitiva, nos encontramos ante un ámbito de aplicación material u objetivo limitado, formalmente cual *numerus clausus*, pero que materialmente es de notable amplitud y generosidad, ya que abarca la práctica totalidad de las materias que, conforme a los Tratados, se encuentran dentro de las competencias normativas de la Unión Europea.

b) La necesaria articulación de los distintos canales de denuncia que deben existir de acuerdo con la Directiva

Conforme se ha anticipado, la Directiva articula un sistema de denuncias por tres cauces distintos (pero, en cierta medida, complementarios): (i) denuncias a través de canales internos ante los órganos competentes designados por las entidades (jurídicas) de los sectores público y privado (arts. 7 a 9 de la Directiva); (ii) denuncias a través de canales externos ante las autoridades (públicas) competentes designadas por los Estados miembros (arts. 10 a 14 de la Directiva); y (iii) revelación pública de información sobre infracciones (p. ej., a través de los medios de comunicación) (art. 15 de la Directiva). Es interesante, sin duda, la opinión manifestada por Mirando Díaz acerca de que "*la nueva Directiva pretende mitigar las posibles deficiencias señaladas en cada modelo* [de denuncia]*, y para ello prevé un sistema de denuncias trifásico, de forma que se configuren canales de denuncia internos (artículos 7-9) —a nivel de la empresa o entidad pública* […]*— y externos (artículos 10 y ss) —que serán aquellos que deban dirigirse hacia un órgano fiscalizador especializado, con un tercer nivel de divulgación pública que actúa como última ratio* […]*—*"[78].

Ya se ha hecho mención y proporcionado alguna explicación, con anterioridad, sobre la denuncia a través de canales internos (*i. e.*, aquellos canales de denuncia que se deben instituir en el seno de la propia organización o entidad, pública o privada, en la que se encuentre integrado o en la que preste servicios el denunciante). Así, como se ha señalado, la Directiva considera que este tipo de canales de denuncia debe tener carácter preferente sobre los otros dos canales de denuncia, por estimarse un medio más adecuado para poner de manifiesto las posibles infracciones del Derecho de la UE, tal y como señala, por ejemplo, el artículo 7.2 de la Directiva ("*Los Estados miembros promoverán la comunicación a través de canales de denuncia interna antes que la comunicación a través de canales de denuncia externa*"). Nos detendremos por ello brevemente ahora en esos dos otros canales de denuncia que recoge la Directiva.

(i) La denuncia a través de canales externos (o, más precisamente, la "*comunicación a través de canales de denuncia externa*") consiste en una comunicación verbal o por escrito en la que se proporcione información sobre infracciones de Derecho de la UE ante las autoridades públicas competentes que debe designar cada Estado

76 El considerando 15 de la Directiva proporciona, en este sentido, una detallada explicación de este tipo de infracciones: "[…] *la protección de los intereses financieros de la Unión relacionados con la lucha contra el fraude, la corrupción y cualquier otra actividad ilegal que afecte a los gastos, la recaudación de ingresos y los fondos o activos de la Unión es un ámbito clave en el que la aplicación del Derecho de la Unión debe reforzarse. También es pertinente reforzar la protección de los intereses financieros de la Unión para la ejecución del presupuesto de la Unión por lo que se refiere a los gastos en que se incurre sobre la base del Tratado constitutivo de la Comunidad Europea de la Energía Atómica (Tratado Euratom). La falta de aplicación efectiva en el ámbito de la protección de los intereses financieros de la Unión, incluida la prevención del fraude y la corrupción a escala nacional, conduce a un descenso de los ingresos de la Unión y un uso indebido de sus fondos, que puede falsear las inversiones públicas, dificultar el crecimiento y socavar la confianza de los ciudadanos en la acción de la Unión* […]".

77 Vid. a este respecto los considerandos 16, 17 y 18 de la Directiva.

78 Javier Miranzo Díaz: "La nueva Directiva de protección del denunciante…", *op. cit.*

miembro a tal efecto. Estas autoridades deberán recibir las denuncias, darles respuesta y "seguirlas", debiendo ser dotadas con los "*recursos adecuados*" para que puedan desarrollar sus funciones (art. 11.1 de la Directiva).

En los términos anticipados, la denuncia externa se plantea como una vía alternativa o complementaria a la denuncia a través de canales internos, pues los denunciantes podrán utilizar los canales de denuncia externa ya sea directamente o tras haber informado de forma pertinente a través de tales canales internos (art. 10 de la Directiva). Estos canales de denuncia —dispone la Directiva— deberán ser diseñados y gestionados por las autoridades competentes de los Estados miembros de forma que:

a) garanticen la exhaustividad, integridad y confidencialidad de la información proporcionada por el denunciante, impidiéndose el acceso a personal no autorizado de la autoridad competente; y

b) permitan el almacenamiento duradero de la información, de conformidad con lo dispuesto en el artículo 18 de la Directiva[79], para que pueda ser utilizada, en su caso, en nuevas investigaciones.

Cabe señalar, por último, que el artículo 13 de la Directiva se ocupa de regular, con singular detalle, la "*Información relativa a la recepción y seguimiento de las denuncias*" que debe ser proporcionada por las autoridades competentes. A este respecto se establece que "*Los Estados miembros velarán por que las autoridades competentes publiquen, en una sección separada, fácilmente identificable y accesible de sus sitios web, como mínimo la información siguiente* [...]"[80].

(ii) La revelación pública, contemplada en el artículo 15 de la Directiva, se entiende como la puesta a disposición del público de información sobre posibles infracciones del Derecho de la UE. Se contempla, en este sentido, como un mecanismo "subsidiario", que podrá utilizar el denunciante cuando se haya agotado la vía de la denuncia a través de canales internos o externos sin que se hayan tomado medidas apropiadas[81], o cuando por determinadas circunstancias no sea conveniente utilizar las otras vías de denuncia[82].

La regulación del régimen de esta revelación pública en la Directiva es sucinta. De forma implícita, parece que el legislador de la UE pretende, con ello, dar un amplio margen de maniobra a los Estados miembros para que,

79 El artículo 18 de la Directiva ("*Registro de las denuncias*") dispone a este respecto, en su apartado primero, que "*Los Estados miembros velarán por que las entidades jurídicas de los sectores privado y público y las autoridades competentes lleven un registro de todas las denuncias recibidas, en cumplimiento de los requisitos de confidencialidad contemplados en el artículo 16. Las denuncias se conservarán únicamente durante el período que sea necesario y proporcionado a efectos de cumplir con los requisitos impuestos por la presente Directiva, u otros requisitos impuestos por el Derecho de la Unión o nacional*".

80 Entre esta información debe encontrarse, necesariamente, la siguiente: "[...] *(a) las condiciones para poder acogerse a la protección en virtud de la presente Directiva; (b) los datos de contacto para los canales de denuncia externa previstos en el artículo 12, en particular, las direcciones electrónica y postal y los números de teléfono para dichos canales, indicando si se graban las conversaciones telefónicas; (c) los procedimientos aplicables a la denuncia de infracciones, incluida la manera en que la autoridad competente puede solicitar al denunciante aclaraciones sobre la información comunicada o proporcionar información adicional, el plazo para dar respuesta al denunciante y el tipo y contenido de dicha respuesta; (d) el régimen de confidencialidad aplicable a las denuncias y, en particular, la información sobre el tratamiento de los datos de carácter personal de conformidad con lo dispuesto en el artículo 17 de la presente Directiva, los artículos 5 y 13 del Reglamento (UE) 2016/679, el artículo 13 de la Directiva (UE) 2016/680 y el artículo 15 del Reglamento (UE) 2018/1725, según corresponda; (e) la naturaleza del seguimiento que deba darse a las denuncias; (f) las vías de recurso y los procedimientos para la protección frente a represalias, y la disponibilidad de asesoramiento confidencial para las personas que contemplen denunciar; (g) una declaración en la que se expliquen claramente las condiciones en las que las personas que denuncien ante la autoridad competente están protegidas de incurrir en responsabilidad por una infracción de confidencialidad con arreglo a lo dispuesto en el artículo 21, apartado 2, y (h) los datos de contacto del centro de información o de la autoridad administrativa única independiente prevista en el artículo 20, apartado 3, en su caso*".

81 *Vid*. considerando 79 de la Directiva: "*Las personas que revelen públicamente infracciones deben poder acogerse a protección en los casos en que, pese a la denuncia interna o externa, la infracción siga sin ser atendida, por ejemplo, cuando la infracción no se ha evaluado o investigado adecuadamente o no se han adoptado medidas correctoras adecuadas. La adecuación del seguimiento debe valorarse con arreglo a criterios objetivos, vinculados a la obligación de las autoridades competentes de valorar la exactitud de las alegaciones y poner fin a cualquier posible infracción del Derecho de la Unión. La adecuación del seguimiento dependerá por tanto de las circunstancias de cada caso y de la naturaleza de las normas que se hayan infringido. En particular, el hecho de que las autoridades hayan decidido que una infracción es claramente menor y que no se requiere ulterior seguimiento, que no sea el archivo del procedimiento, puede constituir un seguimiento adecuado con arreglo a la presente Directiva*".

82 *Vid*. considerando 81 de la Directiva: "*Las personas que revelen directa y públicamente infracciones también deben poder acogerse a protección cuando tengan motivos razonables para pensar que en caso de denuncia externa exista un riesgo de sufrir represalias o sea poco probable que la infracción se trate de manera efectiva, dadas las circunstancias particulares del caso, como que puedan ocultarse o destruirse las pruebas o que una autoridad pueda estar en connivencia con el autor de la infracción o implicada en esta*".

fijando unos estándares mínimos, sean estos quienes regulen los pormenores de la revelación pública como "canal" de comunicación de las denuncias. Es de desear, en este sentido, que nuestro país adopte las necesarias cautelas a la hora de implementar un canal de denuncias que, aunque puede convertirse en una fuente muy valiosa de información, también es altamente susceptible de convertirse con facilidad en un arma de doble filo.

c) El establecimiento de un régimen sancionador *ad hoc* por parte de los Estados miembros

La Directiva obliga a los Estados miembros, en su artículo 23, al establecimiento de "*sanciones efectivas, proporcionadas y disuasorias*" —cuya calificación deberá ser determinada por cada Estado miembro[83]— a las personas, físicas o jurídicas, que:

(i) impidan o intenten impedir las denuncias;

(ii) adopten medidas de represalia contra las personas protegidas por la Directiva;

(iii) promuevan procedimientos abusivos contra las personas protegidas por la Directiva;

(iv) incumplan el deber de mantener la confidencialidad de la identidad de los denunciantes.

Por lo que se refiere al régimen de infracciones que deben ser objeto de sanción por parte de los Estados miembros, la Directiva no se pronuncia de forma expresa sobre la procedencia de imponer sanciones al propio incumplimiento de la obligación de implantar un canal de denuncias adecuado por parte de las distintas entidades, públicas o privadas, sometidas a su ámbito de aplicación. No es seguro si se trata de una omisión deliberada o, por el contrario, de un descuido involuntario por parte del legislador de la UE. No obstante, tal incumplimiento podría entenderse comprendido en la conducta (punible) de "*impedir o intentar impedir las denuncias*", aunque a tal interpretación podría oponerse que se trata de una interpretación extensiva de la norma sancionadora, proscrita en nuestros ordenamiento jurídico-constitucional, por cuanto entraría en conflicto con el principio de legalidad, en sus diferentes dimensiones, que aparece consagrado en el artículo 25.1 de la Constitución española.

En cuanto a los denunciantes, la Directiva también obliga a los Estados miembros al establecimiento, igualmente, de "*sanciones efectivas, proporcionadas y disuasorias*" para aquellos que denuncien con mala fe, esto es, que comuniquen o revelen públicamente información falsa a sabiendas de su falta de veracidad[84].

2.3 · La directiva desde la perspectiva del Derecho penal

2.3.1 · Panorama previo a la publicación de la Directiva

En el ámbito penal, la implantación de un canal de denuncias en el seno de las personas jurídicas para comunicar de manera interna la comisión de conductas potencialmente constitutivas de delitos adquirió importancia con la Ley Orgánica 5/2010, de reforma del Código Penal. Dicha ley introdujo una modificación que supuso un cambio de paradigma en el Derecho penal y en el Derecho procesal penal en España, pues introdujo la posibilidad de atribuir responsabilidad penal a la persona jurídica para determinados delitos, con lo que desapareció de nuestro ordenamiento jurídico el tradicional aforismo *societas delinquere non potest*.

Durante los primeros años de aplicación del régimen de responsabilidad penal de la persona jurídica, se produjo un extenso y rico debate en la doctrina sobre el fundamento de este tipo de responsabilidad. Muy resumidamente, podría decirse que la doctrina se dividía en dos posturas: (i) el sistema de responsabilidad por transferencia o *heterorresponsabilidad*, según el cual la mera comisión del hecho delictivo por la persona física que forma parte de la entidad (p. ej., un empleado) ya implica automáticamente[85], sin más debate, la res-

83 El considerando 102 de la Directiva señala, en su inciso primero, que "*Las sanciones penales, civiles o administrativas son necesarias para garantizar la eficacia de las normas sobre protección de los denunciantes. Las sanciones contra quienes tomen represalias u otras acciones perjudiciales contra los denunciantes pueden desalentar tales acciones* [...]".

84 Continúa señalando el considerando 102 de la Directiva que "[...] *Son necesarias asimismo sanciones contra las personas que comuniquen o revelen públicamente información sobre infracciones cuando se demuestre que lo hicieron a sabiendas de su falsedad, con el fin de impedir nuevas denuncias maliciosas y de preservar la credibilidad del sistema. La proporcionalidad de tales sanciones debe garantizar que no tengan un efecto disuasorio en los denunciantes potenciales*".

85 Siempre y cuando el hecho fuera constitutivo de uno de los delitos susceptibles de generar responsabilidad penal de la persona jurídica y se hubiera cometido en nombre y en beneficio de esta.

ponsabilidad penal de esa entidad[86]; y (ii) el sistema de responsabilidad por el hecho propio o *autorresponsabilidad*, según el cual, para atribuir un delito a la persona jurídica, debe acreditarse la existencia de un *defecto de organización* en ella que haya facilitado o coadyuvado a la comisión del delito por parte de la persona física[87].

Así pues, aquellos que abogaban por el segundo de los sistemas citados —el de la autorresponsabilidad— sostenían que, por aplicación del principio de culpabilidad que rige en el ordenamiento penal, aquellas entidades que hubieran implementado un programa de cumplimiento idóneo para la prevención del hecho delictivo cometido por la persona física no debían responder penalmente de ese hecho. La Ley Orgánica 5/2010, sin embargo, no hacía ninguna referencia a dichos programas de cumplimiento y, por tanto, tampoco señalaba los requisitos que estos debían reunir para ser idóneos para evitar la responsabilidad penal de la persona jurídica. En cualquier caso, tomando como base los estándares internacionales en la materia, la doctrina entendió que uno de los elementos fundamentales de todo sistema de *compliance* era la existencia de un *canal de denuncias*, esto es, de mecanismos internos adecuados para permitir, fomentar, e incluso exigir, que los integrantes de la persona jurídica comuniquen dentro de la entidad la presunta comisión de conductas contrarias a la ética empresarial y a las políticas internas de la empresa, lo que lógicamente incluye las conductas potencialmente constitutivas de delito[88]. Para conseguir ese objetivo, la doctrina coincidía en que el canal de denuncias debía al menos reunir tres rasgos: (i) que sea fácilmente accesible para los integrantes de la entidad y conocido por estos, lo que conlleva la necesidad de difundir adecuadamente la existencia del canal en el seno de la entidad; (ii) que se mantenga la confidencialidad del denunciante, de modo que este tenga la seguridad de que su identidad solo será conocida por las personas encargadas de investigar los hechos y de tomar las decisiones que corresponda; y (iii) que se garantice al denunciante la ausencia de represalias por parte de la entidad por el mero hecho de haber denunciado[89].

En cualquier caso, las dudas sobre la importancia de los citados programas de cumplimiento para la prevención de delitos —también sobre la necesidad de implantar el correspondiente canal de denuncias— fueron disipadas tras la aprobación de la Ley Orgánica 1/2015, de reforma del CP. Dicha ley modificó el artículo 31 bis del CP para, entre otras cosas, aclarar que la persona jurídica estaría exenta de responsabilidad penal si, con carácter previo a la comisión del delito, hubiera implementado un programa de cumplimiento (o, siguiendo la terminología del legislador penal, un "modelo de organización y gestión") adecuado para prevenir delitos de la naturaleza del que fue cometido por la persona física o para reducir de forma significativa el riesgo de su comisión. Además, la citada reforma del CP estableció los requisitos generales que esos programas debían reunir para que fueran susceptibles de exonerar a la persona jurídica de responsabilidad penal.

Pues bien, como era de esperar, uno de esos requisitos consiste en que el programa de cumplimiento imponga la *obligación*, para todos los miembros de la entidad, "*de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención*" (artículo 31 bis.5.4.ª). *El CP no especifica, sin embargo, el procedimiento que las entidades deben establecer internamente como cauce para formular este tipo de comunicaciones. No aclara, por ejemplo, si puede (o debe) establecerse la posibilidad de formular denuncias internas de forma anónima, si es obligatorio mantener la confidencialidad del denunciante y con qué límites, o si debe haber algún tipo de garantía adicional, como la ya mencionada ausencia de represalias contra el denunciante. No obstante, se ha entendido que ese requisito del citado inciso 4.º del apartado 5.º del artículo 31 bis* del CP se refiere a la implantación de un canal de denuncias con los derechos y garantías propios de los estándares internacionales, a los que ya hemos hecho referencia. Y esa ha sido, igualmente, la posi-

86 Esa era la opinión, por ejemplo, de Gonzalo Rodríguez Mourullo: "La responsabilidad penal de las personas jurídicas y los principios básicos del sistema", *Abogados*, septiembre de 2010; o de F. Morales Prats: "La responsabilidad penal de las personas jurídicas (arts. 31 bis., supresión, 33.7, 66 bis., 12, 130.2 CP), en G. Quintero Olivares (dir.): *La reforma penal de 2010: análisis y comentarios*, Cizur Menor: Aranzadi, 2010".

87 Entre otros, E. Bacigalupo Zapater: "Responsabilidad penal y administrativa de las personas jurídicas y programas de 'compliance' (a propósito del Proyecto de reformas del Código Penal de 2009)", *Diario La Ley*, n.º 7442, 9 de julio de 2010; o C. Gómez-Jara Díez: "Fundamentos modernos de la responsabilidad penal de las personas jurídicas. Bases teóricas, regulación internacional y nueva legislación española", Buenos Aires, 2010.

88 Entre otros, A. Nieto Martín: "Investigaciones internas, *whistleblowing* y cooperación: la lucha por la información en el proceso penal", *Diario La Ley*, n.º 8120, 5 de julio de 2013.

89 Estos tres elementos forman parte, como decimos, de las buenas prácticas internacionales en materia de *compliance*. De hecho, son algunos de los requisitos exigidos por la norma *UNE 19601:2017 Sistemas de gestión de compliance penal*.

ción mostrada por la Fiscalía General del Estado en su conocida Circular 1/2016. Literalmente: "*La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención. Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (whistleblower), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos…) sin riesgo a sufrir represalias*"[90].

En definitiva, aunque la existencia de un canal de denuncias en el seno de las entidades no era algo totalmente nuevo en nuestro ordenamiento jurídico[91], no cabe duda de que su generalización en el ámbito empresarial español trae causa de la introducción de la responsabilidad penal de las personas jurídicas.

2.3.2 · Impacto de la Directiva

Como ya se ha expuesto, la Directiva protege a las personas que informen sobre determinadas infracciones del Derecho de la Unión, con independencia de que el Derecho nacional las clasifique como administrativas, penales o de otro tipo.

Pues bien, buena parte de las materias incluidas en el ámbito de aplicación de la Directiva (artículo 2) pueden, a su vez, vincularse a determinadas áreas de riesgo penal. Así, sin perjuicio de que será el legislador español quien decida qué delitos se encuadran en cada una de esas materias, a título de ejemplo pueden relacionarse las siguientes áreas: (i) blanqueo de capitales; (ii) financiación del terrorismo; (iii) delitos contra la Hacienda Pública; (iv) delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores; (v) delitos de descubrimiento y revelación de secretos y allanamiento informático; (vi) daños informáticos; (vii) delitos contra los recursos naturales y el medio ambiente; (viii) delitos relativos a la energía nuclear y a las radiaciones ionizantes; (ix) delitos contra la Administración pública (p. ej., cohecho, tráfico de influencias, malversación); o (x) delitos contra la salud pública.

El legislador podrá extender la aplicación de las medidas de protección de la Directiva a la denuncia de otros delitos no relacionados con las materias enumeradas en el artículo 2 de la Directiva. Ello permitiría armonizar la protección de los denunciantes, independientemente de la infracción penal que comunicaran. En todo caso, se produzca o no esa armonización con ocasión de la transposición de la Directiva, es de esperar que las directrices marcadas en ella en materia de procedimiento y garantías se apliquen de forma generalizada en los canales de denuncia de las entidades. No tendría sentido que el canal de denuncias instaurado en una empresa diferenciara el procedimiento a seguir en función de si el hecho denunciado afecta o no a las materias de Derecho comunitario cubiertas por la Directiva.

Como decíamos, a partir de la introducción de la responsabilidad penal de la persona jurídica en 2010, y especialmente tras la reforma operada por la Ley Orgánica 1/2015, los canales de denuncias se han venido generalizando en el panorama empresarial español, si bien la consecuencia de no haber implementado dichos canales solo aparecerá en caso de que se cometa un hecho delictivo en el seno de la entidad. En otras palabras, la virtualidad de disponer de un programa de cumplimiento conforme a los requisitos previstos en el artículo 31 bis del CP radica en la posibilidad de que la entidad se beneficie de la exención de responsabilidad penal prevista en dicho precepto. De este modo, si no se produce el episodio delictivo, la ausencia del modelo en sí misma no tiene aparejada ninguna consecuencia legal.

Pues bien, como ya exponíamos en el apartado 2.2.2(C) *ut supra*, la implementación de las normas previstas en la Directiva en materia de protección de *whistleblowers* devendrá obligatoria tras su transposición, por lo que será posible la aplicación de sanciones en caso de incumplimiento de dichas normas (vid. apartado 2.2.2.C *ut supra*). Este es, por tanto, el primer efecto que cabe esperar de la Directiva: los programas de cumplimiento para la prevención de delitos existentes hasta la fecha tendrán que ser modificados para adaptarse a la nueva regulación que incorporará la transposición de la Directiva, pues su cumplimiento es imperativo.

90 BOE FIS-C-2016-00001, página 23. Disponible en https://www.boe.es/buscar/doc.php?id=FIS-C-2016-00001.

91 El artículo 50 del Código Unificado de Buen Gobierno de las Sociedades Cotizadas, "Código Conthe", emitido por la Comisión Nacional del Mercado de Valores (CNMV) en 2006, ya señalaba que correspondía al Comité de Auditoría "*establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma confidencial y, si se considera apropiado, anónima las irregularidades de potencial trascendencia, especialmente financieras y contables, que se adviertan en el seno de la empresa*".

Con ello, la Directiva viene a completar la escasa regulación penal existente en España sobre los canales de denuncias y su modo de gestión y funcionamiento.

Puede decirse que, con carácter general, la Directiva sigue el estándar internacional existente hasta la fecha en materia de canal de denuncias y protección de *whistleblowers*. Por ello, la aplicación de la Directiva no parece que vaya a plantear grandes problemas en cuanto a su adecuación a lo exigido en el artículo 31 bis del CP, especialmente teniendo en cuenta la ausencia de una regulación precisa en dicho precepto.

No obstante y sin perjuicio de lo anterior, será conveniente que el legislador español, al transponer la Directiva, tenga en cuenta algunas especificidades del régimen previsto en el artículo 31 bis del CP.

En primer lugar, dicho precepto exige a los integrantes de la persona jurídica que acudan necesariamente al canal de denuncias interno para comunicar posibles riesgos e incumplimientos, mientras que la Directiva ofrece al denunciante distintos medios para informar de la existencia de irregularidades detectadas en el seno de la organización: canales internos, externos o, en determinados casos, a través incluso de la revelación pública. Es decir, podría entenderse que el artículo 31 bis del CP está siendo algo más restrictivo para los derechos de los potenciales denunciantes en la medida en que estaría exigiendo a las entidades que *obligasen* a sus integrantes a utilizar necesariamente el canal de denuncias interno, cuando la Directiva establece que los medios para denunciar son alternativos (si bien fomenta el uso de la denuncia interna en los términos ya expuestos). Así, según la Directiva, es el denunciante el que decide acudir a la vía interna o a la externa para formular su denuncia (incluyendo, insistimos, la revelación pública de los hechos, sin bien con carácter subsidiario y en los supuestos excepcionales ya mencionados en el apartado 2.1.2(C)(i) anterior). No obstante, a nuestro juicio, esta aparente discrepancia no debería tener una gran incidencia en la práctica en la medida en que, a día de hoy, el hecho de que un empleado denuncie los hechos presuntamente irregulares ante las autoridades competentes (denuncia externa) no debería, en sí mismo, ser generador de una sanción disciplinaria por la empresa. Ello es así porque dicho empleado estaría ejerciendo un derecho o, mejor dicho, estaría cumpliendo una obligación, si nos atenemos a lo previsto en los artículos 259[92] y 264[93] de la Ley de Enjuiciamiento Criminal (si bien la sanción aparejada al cumplimiento de esa obligación de denunciar es tan leve que no se aplica en la práctica).

Por otro lado, sobre la función de supervisar el funcionamiento y cumplimiento del modelo de prevención de delitos, el artículo 31 bis.2 del CP establece que debe confiarse dicha función a un órgano de la persona jurídica con poderes autónomos de iniciativa y control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica. En las personas jurídicas de pequeñas dimensiones, esta función podrá ser asumida por el propio órgano de administración. La Directiva, por su parte, hace una recomendación sobre la configuración del órgano encargado de recibir y seguir las denuncias en las entidades de menor tamaño, e indica que esta función se podrá asignar a otro órgano ya existente de la sociedad, siempre que este pueda comunicarse directamente con la dirección de la organización (se ponen algunos ejemplos: un responsable de recursos humanos o de asuntos jurídicos, un responsable financiero, un responsable de auditoría o incluso un miembro del consejo de administración)[94]. De cara a la transposición de la Directiva, sería conveniente que el legislador español aclarase si esas recomendaciones que se formulan en la Directiva son o no compatibles con el hecho de que el artículo 31 bis del CP exija que las denuncias internas

---

92 Artículo 259 LECrim: "*El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal, o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas*".

93 Artículo 264 LECrim: "*El que por cualquier medio diferente de los mencionados tuviere conocimiento de la perpetración de algún delito de los que deben perseguirse de oficio, deberá denunciarlo al Ministerio Fiscal, al Tribunal competente o al Juez de instrucción o municipal, o funcionario de policía, sin que se entienda obligado por esto a probar los hechos denunciados ni a formalizar querella. El denunciador no contraerá en ningún caso otra responsabilidad que la correspondiente a los delitos que hubiese cometido por medio de la denuncia, o con su ocasión*".

94 Considerando 56: "*La elección de las personas o departamentos de una entidad jurídica del sector privado más adecuados para encomendarles la recepción y seguimiento de las denuncias depende de la estructura de la entidad, pero, en cualquier caso, su función debe permitir garantizar la independencia y la ausencia de conflictos de intereses. En las entidades de menor tamaño, podría tratarse de una función dual a cargo de un ejecutivo de la sociedad bien situado para comunicarse directamente con la dirección de la entidad, por ejemplo, un responsable de cumplimiento normativo o de recursos humanos, un responsable de la integridad, un responsable de asuntos jurídicos o de la privacidad, un responsable financiero, un responsable de auditoría o un miembro del consejo de administración*".

sean dirigidas en concreto al órgano interno encargado de vigilar el funcionamiento y observancia del modelo de prevención. A nuestro juicio, es importante garantizar que los procedimientos de denuncia interna de las entidades sigan previendo la necesidad de que el destinatario de la denuncia interna sea dicho "órgano de vigilancia", con o sin filtro previo de un órgano externo en caso de que el canal esté externalizado. Ello es así porque —creemos— el modelo de prevención penal previsto en el CP quiere evitar el riesgo de que las denuncias internas "se pierdan por el camino", es decir, que no se tramiten, por el hecho de formularse ante órganos o puestos de la entidad sin esa función específica de velar por el cumplimiento del programa de prevención de delitos.

Por lo que se refiere a las denuncias anónimas, como ya se ha indicado, la Directiva no establece la obligación de admitirlas, sino que permite que sean los Estados miembros los que decidan si exigen o no a las entidades de los sectores público y privado y a las autoridades competentes la admisión y seguimiento de ese tipo de denuncias.

El anonimato lleva la protección del denunciante un paso más allá de la confidencialidad, al impedir que ni el propio órgano encargado de la tramitación de las denuncias conozca su identidad. No obstante, la admisión y seguimiento de denuncias anónimas sobre hechos supuestamente delictivos puede comprometer el derecho de defensa de la persona afectada por la denuncia, al enfrentarse a una investigación en la que desconoce la identidad de quien le acusa y la procedencia de la evidencia que contra él se aporta.

El Tribunal Supremo ya ha analizado la viabilidad de las denuncias anónimas formuladas ante las autoridades que tienen la obligación de investigar delitos, desde la necesaria salvaguarda del derecho de defensa de los investigados. Siguiendo la jurisprudencia del Tribunal Europeo de Derechos Humanos, el Tribunal Supremo viene admitiendo que las denuncias anónimas sirvan de base para el inicio de una investigación penal, aunque rechaza que puedan ser tenidas como prueba de cargo ni como fundamento para la adopción de medidas cautelares limitativas de derechos fundamentales[95]. No obstante, aunque dicha jurisprudencia haya aceptado la posibilidad de investigar denuncias anónimas, se conceptúa como una reacción frente a una situación excepcional, en la medida en que la Ley de Enjuiciamiento Criminal exige la identificación de la persona o entidad que presente una denuncia o querella ante las autoridades competentes. Dicho de otro modo, si alguien va a presentar una denuncia ante la Policía, el agente que le atienda le requerirá su documento de identidad para poder tramitarla. Cuestión distinta es que, si la Fiscalía u otra autoridad recibe una denuncia anónima (por ejemplo, una carta sin firmar en la que se informe de la comisión de hechos presuntamente delictivos), esa autoridad podrá iniciar una investigación a pesar de desconocer la identidad del autor de esa denuncia, con las limitaciones que impone la jurisprudencia en los términos ya mencionados.

Como se analizará de forma pormenorizada en el apartado 2.4 siguiente, el artículo 24 de la LOPD-GDD permite que se denuncien infracciones de forma anónima a través de los canales de denuncias internos de las entidades de Derecho privado. Sin embargo, la Directiva no solo regula los canales de denuncia internos en entidades del sector privado, sino también las denuncias internas en entidades del sector público y las denuncias externas. De este modo, a la hora de transponer la Directiva, si el legislador español opta por permitir la posibilidad de formular de forma anónima denuncias externas (es decir, ante las "autoridades competentes", lo que lógicamente incluye la Fiscalía, el juez de Instrucción y la Policía), deberá igualmente regular el procedimiento concreto a seguir para presentar este tipo de denuncias, al menos en el ámbito penal. Ello es así porque, como decimos, hasta ahora se plantea como una situación excepcional en la medida en que puede sufrir el derecho de defensa del denunciado, al tener que defenderse de la acusación de alguien cuya identidad desconoce.

De hecho, la Directiva establece una excepción a la regla de la confidencialidad, a efectos precisamente de salvaguardar el derecho de defensa. En concreto, se permite que la identidad del denunciante u otra información sea revelada cuando exista una obligación legal necesaria y proporcionada en el contexto de una investigación o en el marco de un proceso judicial, para garantizar el derecho de defensa de la persona afectada. Así, aunque la identidad del denunciante deberá ser confidencial en el seno de la entidad ante la cual se realice, salvo para determinadas personas (*vid*. apartado 2.4.2.A *infra*), si esa denuncia da lugar a la incoación de un procedimiento (especialmente si es penal), esa obligación

95 *Vid*. sentencias del Tribunal Supremo de 11 de abril de 2013, 6 de noviembre de 2017 y 6 de febrero de 2019, entre otras.

de confidencialidad puede levantarse para salvaguardar el derecho de defensa del denunciado.

Esta posición es coherente con la jurisprudencia actual en materia de testigos protegidos y confidentes, la cual ha tenido ya ocasión de analizar la indefensión que genera en el investigado el hecho de tener que defenderse de hechos imputados por testigos cuya identidad desconoce. Y ello hasta el punto de que, aun tratándose de un testigo protegido (sobre el que, por tanto, ya se ha acreditado una razón de peso para evitar la revelación de su identidad), la jurisprudencia ha restringido a casos excepcionales la posibilidad de mantener el anonimato del testigo en fase de juicio oral. Así lo explica el Tribunal Supremo, en su reciente sentencia de 4 de junio de 2019, con base en jurisprudencia del TEDH:

> "*Teniendo siempre en cuenta que, como se deduce de las reglas generales del proceso penal y de la propia normativa legal, el anonimato del testigo debe ser absolutamente excepcional, pues como ha recordado el TEDH (caso Kostovski vs. Holanda,* sentencia del TEDH, del 20 de noviembre de 1989 (TEDH 1989, 21)*) 'si la defensa desconoce la identidad de la persona a la que intenta interrogar, puede verse privada de datos que precisamente le permitan probar que es parcial, hostil o indigna de crédito. Un testimonio, o cualquier otra declaración contra un inculpado, pueden muy bien ser falsos o deberse a un mero error; y la defensa difícilmente podrá demostrarlo si no tiene las informaciones que le permitan fiscalizar la credibilidad del autor o ponerla en duda* [...]".

Finalmente, otras de las cuestiones que aborda la Directiva con relevancia en el plano penal es la cuestión de si los denunciantes podrían incurrir en responsabilidad penal por la obtención y revelación de información confidencial. A este respecto, entre las medidas de protección frente a las represalias que prevé la Directiva se encuentra la garantía para los denunciantes de que no incurrirán en responsabilidad de ningún tipo en relación con:

(i) la denuncia o revelación pública de información sobre infracciones, a pesar de que el denunciante estuviera sujeto a una obligación de reserva sobre esa información (p. ej., mediante un acuerdo de confidencialidad); y

(ii) la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya de por sí un delito.

Así, desde el punto de vista de la responsabilidad penal, la Directiva distingue entre la difusión o revelación, mediante la denuncia, de información confidencial de la que el denunciante ya tuviera conocimiento —en cuyo caso no existirá responsabilidad penal— y el apoderamiento o acceso ilícito a información confidencial con la finalidad de denunciar la comisión de alguna infracción —supuesto en el que la responsabilidad penal seguirá rigiéndose por el Derecho nacional aplicable—.

De este modo, la Directiva introduce una cuestión que no está prevista de forma expresa en la redacción actual de los delitos de revelación de secretos del Código Penal: la incidencia que la finalidad de denunciar irregularidades puede tener en la responsabilidad penal de quien vulnera sus deberes de confidencialidad (ya sea respecto de información relativa a la intimidad de las personas o de información constitutiva de secreto de empresa).

Sin embargo, esta cuestión no resulta del todo novedosa en la práctica de los Tribunales españoles, ni en nuestra doctrina[96]. Así, los Tribunales entienden que la revelación de información confidencial (revelación de secretos) para denunciar hechos delictivos ante las autoridades competentes no es constitutiva de delito. Tanto la doctrina como la jurisprudencia han esgrimido razones de diversa índole para considerar atípica la revelación de información secreta con la finalidad de denunciar la comisión de hechos delictivos ante las autoridades correspondientes: (i) por entender que la conducta se encuentra amparada por el ejercicio del derecho a denunciar (aplicando la eximente del art. 20.7 CP); (ii) por estimar que el acusado actuó bajo "error de prohibición invencible", por ejemplo en los casos en los que, antes de la revelación, el autor obtuvo asesoramiento legal sobre la licitud de dicha actuación; (iii) por desconocimiento del origen ilícito de los datos difundidos; o (iv) por la ausencia del dolo de "difundir".

96 Entre otros, Ramón Ragués i Vallès: *Whistleblowing. Una aproximación desde el Derecho Penal*, Madrid: Marcial Pons, 2013; o Cristina Rodríguez Yagüe: "La protección de los Whistleblowers en el ordenamiento español", en Luis Arroyo Zapatero y Adán Nieto Martín (coords.): *Fraude y corrupción en el Derecho penal económico europeo. Eurodelitos de corrupción y fraude*, Cuenca: Ediciones de la Universidad de Castilla-La Mancha, 2006, págs. 459-460. En contra de la aplicación del art. 20.7 CP, por entender que no existe ningún deber de denunciar los delitos que se detecten en el seno de la empresa, véase Bernardo del Rosal Blasco: *Manual de responsabilidad penal y defensa penal corporativas*, Madrid: Wolters Kluwer, 2018, págs. 342 y ss.

El ejemplo más relevante es la Sentencia del Tribunal Supremo de 22 de octubre de 2013 (caso de las prótesis mamarias), en la que el Tribunal entendió que la revelación de secretos personales (en el caso concreto, historiales médicos) para denunciar ante las autoridades competentes hechos aparentemente delictivos se encontraba justificada por el cumplimiento del deber general de denunciar delitos, previsto en la Ley de Enjuiciamiento Criminal. Respuestas similares de la jurisprudencia pueden verse en el Auto del Tribunal Supremo de 17 octubre de 2013 o la Sentencia de la Audiencia Provincial de Lleida, Sección 1.ª, de 16 de mayo de 2019.

Otro caso relevante en la jurisprudencia penal sobre esta cuestión es el auto que dictó la Sala de lo Penal de la Audiencia Nacional al denegar la extradición de Hervé Falciani solicitada por las autoridades suizas (Auto de 8 de mayo de 2013). Como es sabido, Hervé Falciani, que trabajaba como informático para una entidad financiera en Suiza, facilitó datos bancarios a la Fiscalía francesa que, al parecer, servirían para acreditar la presunta comisión de fraude fiscal por parte los clientes de la citada entidad. En este sentido, el auto de la Sala de lo Penal de la Audiencia Nacional concluye que, aplicando el Código Penal español, los hechos atribuidos al Sr. Falciani no son constitutivos ni de delito contra la intimidad ni de delito de revelación de secreto de empresa, al no merecer protección jurídica en este caso los secretos revelados por el Sr. Falciani:

> "*Recapitulando, debemos indicar, que en nuestro derecho, el secreto no es un valor o un bien en sí mismo que merezca en sí y por sí mismo ser protegido, sino como elemento puramente instrumental para proteger lo que son auténticos bienes jurídicos merecedores de protección, tales como son la intimidad, la libre competencia, el secreto de empresa, la seguridad del Estado, etc., por ello resulta un elemento imprescindible la licitud de aquella información que se encuentra amparada bajo el secreto, bien sea bajo la protección de la intimidad o bajo la protección del secreto de empresa y, en todo caso, existen intereses superiores que relevan de este secreto y justifican la cesión de la información en favor de determinados sujetos públicos, además de interesados, legitimados para conocer la información, tales como son las autoridades administrativas competentes en materia de defraudación tributaria, y específicamente el Ministerio Fiscal y los Tribunales, en la investigación y persecución de ilícitos penales*".

Aunque la jurisprudencia mencionada ya se ha adelantado a la Directiva en el tratamiento de esta cuestión, deja muchas puertas abiertas e interrogantes que el legislador deberá resolver a la hora de abordar la transposición. Entre otros aspectos, el legislador deberá tener en cuenta que la Directiva no solo ampara a las personas que denuncien ilícitos penales ante las autoridades, sino que protege a todos aquellos que revelen infracciones de cualquier tipo (penales, administrativas, etc., siempre que entren dentro del ámbito material de aplicación), incluso mediante revelación pública.

En definitiva, la Directiva supone un paso más en la protección de los denunciantes y la regulación de los canales de denuncia, siguiendo la tendencia de algunos países europeos, como Italia con la Ley 179/2017 —que ya ha supuesto la imposición de la primera sanción por las represalias sufridas por un denunciante en el ámbito público— o Francia con la Ley n.° 2016-1691, más conocida como Ley *Sapin* II —que establece sanciones para las empresas que no prevean procedimientos y canales internos de denuncia en sus programas de *compliance*—.

No obstante y sin perjuicio de lo anterior, la Directiva no aborda dos medidas que, aunque polémicas, han sido consideradas como mecanismos eficaces para fomentar el uso de los canales de denuncias internos. Nos referimos a (i) la posibilidad de eximir de responsabilidad al *whistleblower* que denuncia la conducta infractora cometida por sus superiores o compañeros, pero en la que el propio denunciante tuvo algún tipo de participación; y (ii) la posibilidad de que los Estados ofrezcan a los *whistleblowers* recompensas económicas por el hecho de haber denunciado la conducta irregular.

En relación con la primera de las cuestiones —esto es, la relativa a la introducción de un mecanismo equivalente a los *leniency programmes* o "programas de clemencia" antes mencionados (vid. apartado 2.2.1.A *ut supra*)—, no existe ninguna previsión similar en el ámbito penal. En efecto, la confesión es considerada por el CP como una circunstancia *atenuante* de la responsabilidad penal[97] y no como una circunstancia eximente. Por ello, en puridad, el Ministerio Fiscal estaría obligado a ejercitar la acción penal contra el *whistleblower* confeso, en virtud del principio de legalidad que rige su actuación

97 Artículo 21.4.ª: "*Son circunstancias atenuantes:* [...] *3ª La de haber procedido el culpable, antes de conocer que el procedimiento judicial se dirige contra él, a confesar la infracción de las autoridades*".

conforme a lo previsto en el artículo 6 del Estatuto Orgánico del Ministerio Fiscal (Ley 50/1981, de 30 de diciembre). Ahora bien, en la práctica no es raro que los fiscales y los jueces penales tengan una actitud benevolente frente a la persona que denuncia (y, a la vez, confiesa), lo que en ocasiones se traduce en la absolución del denunciante por entender que cometió los hechos como consecuencia de la autoridad que sus superiores ejercían sobre él (aunque, obviamente, ese análisis deberá hacerse atendiendo siempre al caso concreto).

Por lo que se refiere a la segunda de las medidas citadas —la introducción de un sistema de recompensa económica para el *whistleblower*— tampoco existe una regulación al respecto en el ámbito penal. De hecho, tal y como señala Ragués i Vallés[98], el único ejemplo de recompensa a *whistleblowers* presente en nuestro ordenamiento es el artículo 48 de la Ley 33/2003, de Patrimonio de las Administraciones Públicas, según el cual:

> "*A las personas que, sin venir obligadas a ello por razón de su cargo o funciones promuevan el procedimiento de investigación denunciando, con los requisitos reglamentariamente establecidos, la existencia de bienes y derechos que presumiblemente sean de titularidad pública, se les abonará como premio el diez por ciento del valor de los bienes o derechos denunciados, siempre que el procedimiento concluya con su incorporación al Patrimonio del Estado y esta incorporación no sea revocada posteriormente*".

En el ámbito de la Unión Europea, el artículo 32.4 del Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado, dispone que "*los Estados miembros podrán prever, de acuerdo con la normativa nacional aplicable, la concesión de incentivos económicos a las personas que ofrezcan información relevante sobre posibles infracciones del presente Reglamento, siempre que esas personas no estén sometidas a otras obligaciones legales o contractuales previas de facilitar tal información, que esta sea nueva y que dé lugar a la imposición de una sanción administrativa o penal, o a la adopción de otra medida administrativa por infracción del presente Reglamento*". No obstante, hasta la fecha, ninguno de los Estados miembros ha hecho uso de esta posibilidad[99].

Como es sabido, el país referente en este tipo de incentivos es Estados Unidos, que introdujo por primera vez el sistema de recompensas a *whistleblowers* a través de la *False Claims Act* de 1863, cuyo objetivo era combatir el fraude en el ámbito administrativo[100]. Asimismo, existen diversas leyes sectoriales que prevén recompensas para los *whistleblowers*, entre las que destaca la *Dodd-Frank Act*, de 21 de julio de 2010 (oficialmente, *Dodd–Frank Wall Street Reform and Consumer Protection Act*). Esta Ley introdujo un sistema de recompensas para *whistleblowers* que denunciasen a la *Securities and Exchange Commission* irregularidades cometidas en el ámbito financiero. Hasta la fecha, la recompensa más elevada ha sido de 250 millones de dólares a un *whistleblower* que se acogió a la *False Claims Act* en 2012[101].

Si bien este modelo ha sido implantado en otros países[102], a nuestro juicio es razonable que la Directiva no se haya pronunciado sobre esta cuestión, dejándolo así al arbitrio de cada Estado miembro (recordemos que la Directiva se conceptúa como una norma de mínimos, por lo que cada Estado podrá introducir mecanismos adicionales de fomento de las denuncias). Y decimos que es razonable porque este sistema de recompensa ha sido objeto de muchas críticas. En concreto, entre los argumentos esgrimidos en su contra destacan (i) la menor credibilidad que se atribuye al denunciante, quien puede estar más interesado en obtener la recompensa que en transmitir de forma fidedigna los hechos que cono-

98 Ramón Ragués i Vallès: *Whistleblowing. Una aproximación desde el Derecho penal*, op. cit., pág. 56.

99 En este sentido, Dimitrios Kafteranis: "Rethinking financial rewards for whistle-blowers under the proposal for a Directive on the protection of whistle-blowers reporting breaches of EU law", *Nordic Journal of European Law*, vol. 2. n.º 1, 2019, pág. 42.

100 Jacob M. Howard, el senador que introdujo la ley, justificaba el sistema del siguiente modo: "*I have based the provision upon the old-fashioned idea of holding out a temptation, and 'setting a rogue to catch a rogue,' which is the safest and most expeditious way I have ever discovered of bringing rogues to justice*" (citado en Stephen Kohn: *The new whistleblower's handbook: a step-by-step guide to doing what's right and protecting yourself* Globe Pequot, Guiltord, Connecticut, 2017, pág. 71).

101 Datos extraídos de Jason Zuckerman y Matthew Stock: *What is a whistleblower reward?*, disponible en https://www.zuckermanlaw.com/sp_faq/what-is-a-whistleblower-reward/.

102 Así, por ejemplo, en Canadá, la *Ontario Securities Commission* concedió en 2019, por primera vez en su historia, una recompensa de 7,5 millones de dólares canadienses a tres personas que denunciaron diversos incumplimientos de la normativa de mercados de valores (*vid*. "Ontario market watchdog pays $7.5 million to three whistleblowers in Canada's first reward for tips", *Financial Post*, 27 de febrero de 2019, disponible en https://business.financialpost.com/news/fp-street/ontarios-market-watchdog-to-pay-7-5-million-to-three-whistleblowers). Otros países con sistemas de recompensa a *whistleblowers* son Corea del Sur, Ghana, Hungría y Pakistán (datos extraídos del informe de *Whisteblower reward programmes*, de 27 de septiembre de 2018, disponible en https://knowledgehub.transparency.org/assets/uploads/helpdesk/Whistleblower-Reward-Programmes-2018.pdf).

ce[103]; (ii) la generación de un incentivo en el seno de las empresas para inducir a la comisión de infracciones con el fin denunciarlas posteriormente[104]; y (iii) el riesgo de que, al existir un incentivo tan alto para la delación, ello deteriore las relaciones personales dentro de las organizaciones[105].

Así pues, aun habiendo dejado al margen las cuestiones ya mencionadas de los programas de clemencia y de recompensa económica, tal y como hemos venido exponiendo en el presente trabajo, la Directiva supone un decidido paso hacia adelante en la protección del *whistleblower*, que a buen seguro implicará la correspondiente adaptación de los programas de cumplimiento para la prevención de delitos ya implantados en muchas entidades del ámbito empresarial español.

2.4 · La Directiva desde la perspectiva del Derecho de la protección de datos

2.4.1 · Panorama previo a la publicación de la Directiva

La protección de los datos personales de los interesados cuya información personal se incluye en las denuncias vertidas en los canales de *whistleblowing* y, en particular, la protección de la identidad y los datos personales de los denunciantes son esenciales para que los sistemas de denuncias generen confianza a los *whistleblowers* y, por lo tanto, alienten su uso.

La normativa aplicable en España que protege este derecho —la protección de los datos personales— es el Reglamento (UE) 2016/679 General de Protección de Datos 106 (el "RGPD") y la LOPDGDD, la norma local española. Aunque el RGPD no regula de forma expresa los tratamientos de datos relacionados con los canales de *whistleblowing*, la LOPDGDD —que entró en vigor con anterioridad a la publicación de la Directiva— dedica su artículo 24[107] a regular de forma específica cómo deben aplicarse las reglas y principios de la protección de datos a los tratamientos relacionados con los sistemas de denuncias.

Hasta la entrada en vigor de la LOPDGDD y del RGPD solo existían pronunciamientos de autoridades competentes de protección de datos sobre esta materia. En particular, la autoridad europea de protección de datos —el Grupo de Trabajo del

103 *Vid*., en este sentido, el informe de la Financial Conduct Authority y de la Prudential Regulation Authority del Reino Unido, *Financial Incentives for Whistleblowers*, de julio de 2014, disponible en https://www.fca.org.uk/publication/financial-incentives-for-whistleblowers.pdf. *Vid.* también el informe de Transparency International *Whisteblower reward programmes*, de 27 de septiembre de 2018, disponible en https://knowledgehub.transparency.org/assets/uploads/helpdesk/Whistleblower-Reward-Programmes-2018.pdf.

104 *Vid*., en este sentido, el informe de la Financial Conduct Authority y de la Prudential Regutlation Authority del Reino Unido, y el informe de Transparency International, *ut supra*.

105 *Vid*. a este respecto el repaso de los argumentos, a favor y en contra, que hace Ramón Ragués i Vallès, *op.cit.*, pp. 57-59. En esta misma línea, Kafteranis sostiene que el sistema de recompensas no ha tenido éxito en Europa por los recuerdos de las delaciones de las épocas nazi y soviética. *Vid.* Dimitros Kafteranis, *op. cit.*, p. 49.

106 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

107 El artículo 24 de la LOPDGDD señala lo siguiente: "*1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.*

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica. Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

5. Los principios de los apartados anteriores serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas".

Artículo 29[108] (el "GT29")— publicó el Dictamen 1/2006[109] sobre la aplicación de las normas de la Unión Europea relativas a la protección de datos en el contexto de los programas internos de denuncia (el "Dictamen 1/2006"). Posteriormente, el Gabinete Jurídico de la Agencia Española de Protección de Datos (la "AEPD") también publicó un informe[110] sobre la creación de sistemas de denuncias internas en las empresas (el "Informe 0128/2007"). Aunque con la entrada en vigor del actual marco normativo las citadas directrices no han sido actualizadas, otras autoridades sí han publicado guías sobre esta materia en fechas posteriores teniendo ya en cuenta el RGPD. Entre otras autoridades, el Supervisor Europeo de Protección de Datos ("SEPD") publicó un informe[111] sobre cómo debían tratarse los datos personales en los sistemas de denuncias habilitados en las instituciones y organismos de la UE (el "Informe del SEPD"). Asimismo, la autoridad de protección de datos francesa (el "CNIL[112]") aprobó una guía[113] (la "Guía del CNIL") al respecto. Todos estos pronunciamientos y, en particular el del SEPD y el del CNIL, pueden servir para contextualizar, al menos desde un punto de vista conceptual, el artículo 24 de la LOPDGDD y, así, intentar despejar algunas de las dudas que plantea dicho precepto cuando se pretende conjugar el cumplimiento de las obligaciones impuestas por dicho precepto con la implementación práctica de un canal de denuncias.

A continuación, se sintetizan los requisitos que impone la normativa de protección de datos y, en particular, el artículo 24 de la LOPDGDD a las entidades que implementan un canal de *whistleblowing* con el fin de dar cumplimiento al principio de responsabilidad proactiva (*accountability*) y que los responsables del tratamiento diseñen un sistema de denuncias que desde el inicio y por defecto (*privacy by design and by default*) esté alineado con la normativa de protección de datos.

a) Bases jurídicas del tratamiento

El primer requisito exigido por la norma para poder tratar datos personales es que el responsable del tratamiento compruebe que existe una base jurídica, de entre las recogidas en el artículo 6 del RGPD, para tratar dichos datos. Entre estas, las dos bases jurídicas que podrían tener cabida para legitimar el tratamiento de datos incluidos en las denuncias serían, o bien que exista una norma que obligue al responsable del tratamiento a implementar un canal de *whistleblowing* (art. 6.1.c del RGPD), o bien que sea de aplicación una norma que autorice (*i. e.*, no obligue) —en virtud del artículo 6.1.f del RGPD— la instalación de dicho sistema (p. ej., que al responsable le sean de aplicación obligaciones genéricas de vigilancia de determinadas conductas).

Sin perjuicio de lo anterior, hay que tener en cuenta que a través de los canales de denuncias se podrían tratar datos especialmente protegidos. Entre otros, en las denuncias es habitual que se incluyan datos relacionados con presuntas comisiones de delitos, datos de orientación sexual de compañeros de trabajo, datos de salud del sujeto denunciado o datos de afiliación sindical del denunciante. Dado que los datos especialmente protegidos gozan de un rango de protección mayor, hay que revisar las bases jurídicas que se aplican —de forma exclusiva— a los tratamientos relativos a esta tipología de datos. Dichas bases de legitimación se encuentran reguladas en los artículos 9[114] y 10 del RGPD y en los artículos 9 y 10 de la LOPDGDD. Sobre dichos pre-

108 El GT29, con la aplicación del RGPD, fue sustituido por el Comité Europeo de Protección de Datos. El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos (SEPD).

109 Grupo de Trabajo del Artículo 29: *Dictamen 1/2006 sobre la aplicación de las normas de la Unión Europea relativas a la protección de datos a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros*, Bruselas, 1 de febrero de 2006. Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

110 Agencia Española de Protección de Datos: *Informe del gabinete jurídico n.º 0128/2007 sobre la creación de sistemas de denuncias internas en las empresas*.

111 Supervisor Europeo de Protección de Datos Personales: *Guidelines on processing personal information within a whistleblowing procedure*, publicadas el mes de julio de 2016 y actualizadas en diciembre de 2019. Disponible en https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en.

112 *Commission Nationale de l'Informatique et des Libertés*.

113 CNIL: *Relatif aux traitements de donness a caractere personnel destines a la mise en oeuvre d'un dispositif d'alertes professionnelles*, 10 de diciembre de 2019, disponible online (solo en francés): https://www.cnil.fr/sites/default/files/atoms/files/referentiel-alertes-professionnelles_decembre-2019.pdf.

114 La base jurídica que se aplicaría al tratamiento de datos especialmente protegidos en el contexto de un canal de denuncias sería el artículo 9.2.f del RGPD, que permite tratar dichos datos "*cuando el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial*".

ceptos cabe destacar que el artículo 10 de la LOPDGDD (en línea con el art. 10 del RGPD) señala que el tratamiento de infracciones penales "*solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica* [la LOPDGDD] *o en otras normas de rango legal*". Por lo tanto, las compañías solo podrán tratar datos sobre infracciones o antecedentes penales si existe una norma con rango de ley (europea o local) que autorice dicho tratamiento.

b) Principio de minimización del dato

Existe un principio básico en materia de protección de datos, conocido como el principio de la minimización del dato (art. 5.1.c del RGPD), que establece que solo se deben tratar aquellos datos que sean "*adecuados, pertinentes y limitados a lo necesario*" en relación con el fin con el que se pretenden tratar. Para que los responsables de los canales de denuncias cumplan con dicho principio, deben especificar con claridad —en sus políticas de privacidad— qué tipos de conductas pueden ser objeto de denuncia. Además, los responsables del tratamiento deberían advertir a los *whistleblowers* sobre la prohibición de incluir datos excesivos o no necesarios para denunciar un determinado hecho. En este sentido, tal y como recomiendan el SEPD[115] y el CNIL[116], en el caso de que se vertiesen denuncias que nada tuvieran que ver con el ámbito que pretende cubrir un determinado sistema de denuncias, estas deberían ser suprimidas por los responsables.

c) Admisibilidad de las denuncias anónimas

Hasta la entrada en vigor de la LOPDGDD, la AEPD[117] había prohibido el envío de denuncias anónimas en los canales de *whistleblowing* en su Informe 0128/2007, en contraposición a lo que ocurría en otros países europeos[118]. Por ello, la principal novedad del artículo 24 de la LOPDGDD fue el reconocimiento de la licitud de las denuncias anónimas en España. En este sentido, el artículo 24.1 señala lo siguiente: "*será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable*".

Sin perjuicio de que el artículo 24.1 de la LOPDGDD abra la posibilidad de que se traten denuncias anónimas, desde una perspectiva de protección de datos, es recomendable que el *whistleblower* se identifique. De ahí que sea necesario que las entidades inviten a los denunciantes a que no preserven su anonimato. Esta interpretación nace del tenor literal del citado precepto, tal y como sostuvo Jesús R. Mercader Uguina[119], que al respecto arguyó que el artículo 24.1 de la LOPDGDD, "*por su estricta literalidad, no parece admitir de manera general* [las denuncias anónimas]*, sino solo en la medida en que lo exija el buen funcionamiento del sistema de información de denuncias internas*". En este mismo sentido, la Guía del CNIL[120] indica que las organizaciones deben proponer o, incluso, imponer que el denunciante se identifique. Asimismo, el SEPD —en sus *Directrices sobre Whistleblowing*[121]— aboga por esta misma opción con el fin de evitar el abuso y el uso indiscriminado de los canales de denuncias y para permitir, asimismo, la efectiva protección de los *whistleblowers* contra posibles represalias. Además, el SEPD añade que la identificación del denunciante permite que sea posible recabar más información sobre los hechos denunciados que pueda ser relevante para la resolución del conflicto.

115 SEPD: *Guidelines on processing personal information within a whistleblowing procedure*, pág. 7: "*A good practice is to implement a general recommendation, for example in the internal rules of procedure, for those handling whistleblowing files to remind them to respect the rules on data quality*".

116 CNIL: *Guía del CNIL*, pág. 8: "*Les données relatives à une alerte considérée par le responsable du traitement comme n'entrant pas dan le champ du dispositif, sont détruites sans délai ou anonymisées*".

117 AEPD: *Informe 0128/2007*: "*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*".

118 *Vid. ut supra*, sección 2.2.1 de este trabajo.

119 Jesús R. Mercader Uguina: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Madrid: Francis Lefebvre, 26 de abril de 2019 (3.ª edición).

120 CNIL: *Guía del CNIL*, pág. 6: "*Un dispositif d'alertes professionnelles peut imposer ou proposer que l'auteur de l'alerte s'identifie. Si l'émetteur de l'alerte professionnelle doit s'identifier, son identité est traitée de façon confidentielle par l'organisation ou les personnes chargées de la gestion des alertes. Il est toutefois recommandé que l'organisme n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme, étant entendu qu'une alerte anonyme est une alerte dont l'auteur n'est ni identifié ni identifiable*".

121 SEPD: *Directrices sobre Whistleblowing*, pág. 6: "In principle, whistleblowing should not be anonymous. *Whistleblowers should be invited to identify themselves not only to avoid abuse of the procedure but also to allow their effective protection against any retaliation. This will also allow better management of the file if it is necessary to gather further information*".

d) Información sobre el canal de denuncias

La obligación por antonomasia de la normativa de protección de datos —regulada en los artículos 13 y 14 del RGPD y el artículo 11 de la LOPDGDD— es que los titulares de los datos han de ser informados, entre otras cosas, sobre quién está tratando sus datos personales, con qué finalidad y durante cuánto tiempo.

En este sentido, el artículo 24.1 de la LOPDGDD establece que "*Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información*". Respecto del modo de dar cumplimiento a dicho deber, cabe preguntarse si sería suficiente —para los responsables del canal— solo con informar a los afectados —de forma genérica— acerca de la existencia del canal (tal y como únicamente exige el citado artículo) o si dicho deber de información implicaría, a su vez, informar a los afectados sobre la recepción de una denuncia en la que se incluyan sus datos personales. Por otro lado, el citado artículo no concreta en qué momento debe proporcionarse dicha información.

Con el fin de arrojar algo de claridad sobre estas cuestiones, cabe acudir a los pronunciamientos de las autoridades en materia de protección de datos citados con anterioridad. En este sentido, el GT29, la AEPD, el CNIL y el SEPD en sus respectivas directrices concluyeron —de forma unívoca— que los titulares de los datos personales debían ser informados no solo sobre la existencia del canal de denuncias, sino también sobre el tratamiento de sus datos personales en relación con la denuncia correspondiente en la que se vean involucrados (directa o indirectamente). En concreto, el SEPD en sus *Directrices sobre Whistleblowing* señala que la información ha de ser facilitada en dos fases[122]. En una primera fase se deberá informar sobre la implementación del canal y, adicionalmente (en una segunda fase), cuando se reciba una denuncia, se deberá informar de ello a cada uno de los afectados por dicha denuncia —incluyendo al denunciante, testigos, terceras partes (por ejemplo, compañeros citados en la denuncia) y al denunciado—.

Esta interpretación encaja perfectamente con los preceptos que regulan el deber de información en el marco de protección de datos aplicable en la actualidad (*i. e.*, el art. 13 —aplicable a los casos en los que los datos se obtengan directamente de los interesados— y el art. 14 del RGPD —que será de aplicación a aquellos supuestos en los que estos no se obtengan de los interesados—). Ello se debe a que dichas normas exigen que los responsables del tratamiento pongan a disposición de los interesados una información muy exhaustiva sobre el tratamiento de datos que pretenden llevar a cabo (por ejemplo, indicar qué tipología de datos se tratan y a quién van a ser cedidos). De ahí que sea razonable concluir que, con la mera advertencia de que existe un canal de denuncias, tal y como únicamente exige el art. 24.1 de la LOPDGDD, no se agote el cumplimiento del deber de información.

Aclarado el hecho de que los responsables del tratamiento han de informar a los afectados no solo sobre la existencia del sistema de *whistleblowing*, sino también sobre cualquier denuncia en la que se viesen involucrados, surge la duda de cuándo se debería facilitar dicha información. Dado que el artículo 24.1. de la LOPDGDD tampoco se pronuncia sobre esta cuestión, cabe acudir de nuevo a la regulación general sobre el deber de informar (*i. e.*, los artículos 13 y 14 del RGPD). Al respecto, el artículo 13.1 del RGPD (aplicable a aquellos casos en los que los datos se obtengan directamente de los interesados) indica que los interesados deben ser informados sobre el tratamiento de sus datos "*en el momento en que estos se obtengan*". Para los supuestos en los que no se obtengan los datos directamente de los interesados (p. ej., en el caso de los denunciados y terceros, ya que los datos son aportados por el denunciante), el artículo 14.3.a[123] del RGPD señala que los afectados deben ser informados cuanto antes y, en todo caso, en el plazo de un mes desde que sus datos sean recabados. No obstante, en el contexto de los canales de denuncias,

122 SEPD: *Directrices sobre Whistleblowing*, págs. 7 y 8: "*Information on whistleblowing procedures should be provided to the individuals in a very prominent way, which will involve a* two-step *procedure. While placing a data protection notice on the website (or within a public or internal-facing document) is encouraged, the EDPS* does not *consider this* sufficient*, as the information could be overlooked. All individuals affected by a whistleblowing procedure should be directly provided with a specific data protection notice as soon as practically possible, for example by email. Affected individuals will usually include whistleblowers, witnesses, third parties (members of staff or others that are merely quoted) and the person(s) against whom the allegations has been made*".

123 El artículo 14 del RGPD señala lo siguiente: "*3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2: a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos; b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez*".

hay que tener en cuenta que las investigaciones iniciales, sobre si una determinada denuncia debe ser investigada o no, pueden prolongarse durante un plazo máximo de tres meses (en virtud del art. 24.4[124] de la LOPDGDD). En este sentido, facilitar información sobre la denuncia a los afectados (p. ej., al incriminado) antes de que se decida si procede investigar una denuncia o no (p. ej., el plazo de un mes establecido en el art. 14.3.a del RGPD) podría "*imposibilitar u obstaculizar*" el curso de la investigación (arts. 14.5.b[125] y 23 del RGPD). De acuerdo con lo anterior cabría concluir que —como regla general— los responsables del tratamiento deberían informar a los afectados tan pronto como se haya decidido sobre la procedencia de investigar una determinada denuncia y, en todo caso, en un plazo máximo de hasta tres meses a contar desde la fecha en la que se recibió la correspondiente denuncia (en virtud del art. 24.4 de la LOPDGDD). Sin perjuicio de ello, excepcionalmente, si el responsable del tratamiento considerase que informar sobre la existencia de una determinada denuncia podría obstaculizar una investigación, podría posponer —en virtud del artículo 14.5.b del RGPD— el cumplimiento de dicho deber.

Otra de las particularidades del deber de informar —en el contexto de los canales de denuncias— es que, aunque el artículo 14 del RGPD exige que los afectados sean informados de la procedencia de sus datos, de acuerdo con el artículo 16 de la Directiva y el artículo 24.3[126] de la LOPDGDD —como regla general— la identidad del denunciante no debe ser revelada al resto de afectados (*i. e.*, denunciado y terceros mencionados en la denuncia) con el fin de preservar sus datos confidenciales. Esta excepción al cumplimiento del deber de información fue destacada por Jesús R. Mercader Uguina[127], que sostuvo que "[...] *tal derecho del incriminado encuentra una limitación importante en cuanto al acceso a la identidad del denunciante, puesto que se considera que 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*".

e) Plazos máximos para tratar las denuncias

El RGPD, en su artículo 5.1.e, señala que los datos personales no deben conservarse "*más tiempo del necesario para los fines del tratamiento*". Trasladando este principio al contexto de los sistemas de *whistleblowing*, el artículo 24.4 de la LOPDGDD establece que los datos de quien formule la comunicación y de los empleados y terceros deberán tratarse en el sistema de denuncias "únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados". Además, dicho artículo señala que "*En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica*". Por ello, los responsables del tratamiento solo estarían habilitados a tratar datos personales dentro del canal de denuncias durante el tiempo imprescindible para determinar si la denuncia va a ser investigada o no y, en todo caso, solo podrían tratar las denuncias durante un máximo de tres meses desde la fecha en que estas hubieran sido incluidas en el canal. Las denuncias que pasen a ser investigadas solo se podrán conservar dentro del canal con el único fin de "*dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica*" (art. 24.4 de la LOPDGDD). El periodo máximo —de tratamiento de datos personales dentro de sistemas de *whistleblowing*— expuesto difiere del sugerido por otras autoridades de protección de datos —como el

124 El artículo 24.4. de la LOPDGDD señala: "*4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.*
En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica".

125 El artículo 14.5.b) del RGPD señala: "*5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:* [...] *b)* [...] *o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información* [...]".

126 El artículo 24.3 de la LOPDGDD señala: "*3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado*".

127 Jesús R. Mercader Uguina: *Protección de datos y garantía de los derechos digitales...*, *op. cit.*, pág. 196.

SEPD[128], el CNIL[129] o el GT29[130]— que recomiendan que las denuncias no sean mantenidas dentro de dicho canal más de dos meses a contar desde que se haya finalizado la investigación preliminar sobre la procedencia de tramitar la denuncia (si bien, estas autoridades no especifican un plazo máximo para decidir si la denuncia va a ser investigada o no, tal y como hace la AEPD).

Sin perjuicio de lo anterior, en relación con las denuncias que pasen a ser investigadas, el art. 24.4. de la LOPDGDD señala que —como no podía ser de otra manera— podrán seguir siendo tratadas, en un sistema lógico distinto, por el órgano al que corresponda la investigación de los hechos denunciados sin que se conserven en el propio sistema de información de denuncias internas. Sin perjuicio de ello, el SEPD[131] insta a que —antes de que el órgano o equipo correspondiente investigue los hechos— cualquier dato que no sea necesario para la investigación sea eliminado de la denuncia con el fin de cumplir con el principio de minimización del dato.

Por el contrario, todas aquellas denuncias que no estén relacionadas con el ámbito de protección del canal deberían ser suprimidas o anonimizadas[132] por el responsable del tratamiento inmediatamente, tal y como sostiene el CNIL[133]. En este mismo sentido, de acuerdo con el artículo 24.4. de la LOPDGDD, también las denuncias "*a las que no se haya dado curso*" (*i. e.*, que no pasen a ser investigadas por cualquier motivo) deberían ser anonimizadas si se pretenden mantener en el sistema de denuncias con el fin de dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica.

En relación con esta obligación de anonimizar los datos de las denuncias, cabe aclarar que la anonimización es un proceso mediante el cual los datos anonimizados se transforman en información que no permite reidentificar a la persona física a la que pertenecen (p. ej., cuando se indica que "*un empleado del área de negocio ha infringido una norma interna*"). Sin embargo, el proceso de seudonimización[134], que muchas se confunde con el de anonimización, sí permitiría —aunque de una forma indirecta— llegar a saber quién es la persona física a la que pertenece la información que se le asocia (p. ej., cuando se señala que "*el empleado número 95 ha infringido una norma interna*"). Esta distinción es importante, ya que el RGPD establece que a la información agregada o anonimizada no le es de aplicación la normativa de protección de datos, mientras que a la seudonimizada, sí. No obstante, ello no quiere decir que exista un "cheque en blanco" para anonimizar los datos y tratarlos con los fines que una compañía desee. Al respecto, la AEPD ha puntualizado que la anonimización es un tratamiento en sí mismo[135]. Ello implica que las compañías necesitarían una base jurídica para anonimizar esos datos e informar a los afectados sobre dicho tratamiento en todo caso[136]. Ade-

128 SEPD: *Directrices sobre Whistleblowing*, pág. 11: "*In any case, personal information should be deleted promptly and usually within two months of completion of the preliminary assessment, since it would be excessive to retain such sensitive information*".

129 CNIL: *Guía del CNIL*, pág. 8: "*Lorsqu'aucune suite n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées par l'organisation chargée de la gestion des alertes, dans un délai de deux mois à compter de la clôture des opérations de vérification*".

130 GT29: *Dictamen 1/2006*, pág. 12: *Personal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report.*

131 SEPD: *Directrices sobre Whistleblowing*, pág. 10: "*Personal information that is not relevant to the allegations should not be further processed (see section 4) and deleted with undue delay*".

132 La AEPD ha publicado unas guías sobre cómo se tienen que llevar a cabo los procesos de anonimización: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, disponible en https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf.

133 CNIL: *Guía del CNIL*, pág. 8: "*Lorsqu'aucune suite n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées par l'organisation chargée de la gestion des alertes, dans un délai de deux mois à compter de la clôture des opérations de vérification*".

134 El RGPD define en su art. 4.5. la seudonimización como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*".

135 AEPD: *Informe de su Gabinete Jurídico n.º 195/2017*, sección VIII, disponible en https://www.aepd.es/es/documento/2017-0195.pdf: "[...] *tanto la anonimización como la seudonimización de los datos personales llevarán aparejada la existencia de dos tratamientos sucesivos: el que supone la propia anonimización o seudonimización a partir de los datos personales de que dispone el responsable y el que se lleve a cabo posteriormente con los datos ya anonimizados o seudonimizados.* La diferencia entre ambos supuestos estribará en el hecho de que mientras la normativa de protección de datos no será de aplicación a este segundo tratamiento si los datos han sido anonimizados, sí resultará aplicable en caso de que se haya producido únicamente una seudonimización".

136 AEPD: *Informe de su Gabinete Jurídico n.º 195/2017*, sección VIII, disponible en https://www.aepd.es/es/documento/2017-0195.pdf: "*En todo caso, como se ha indicado para los supuestos anteriormente indicados, será preciso informar a los interesados acerca de los tratamientos que van a tener lugar y garantizar el adecuado ejercicio por aquéllos de su derecho de oposición, al operar éste, según el artículo 21 del reglamento, en los supuestos en que el tratamiento se funde en la regla del equilibrio de derechos e intereses prevista en el artículo 6.1 f) del reglamento*".

más, la AEPD publicó una guía[137] sobre los procesos de anonimización en la que se concluía que, dada la rápida evolución de la tecnología (p. ej., la evolución de la computación cuántica), hay que tener en cuenta que los procesos realizados en la actualidad podrían —en un breve lapso de tiempo— no ser definitivos e irreversibles. Por ello, la AEPD recomienda que los procesos de anonimización sean revisados periódicamente y que se evalúen (incluso realizando las evaluaciones de impacto) los posibles nuevos riesgos que puedan surgir como consecuencia de diferentes factores, riesgo residual de datos anonimizados, nuevas fuentes de datos a cruzar, nuevas tecnologías, etc.[138]. En este sentido, algunos de los aspectos que deben tener en cuenta las compañías si comparten esta información con terceros o empresas del grupo, tal y como recomienda la AEPD, son los siguientes[139]: a) la suscripción de acuerdos de confidencialidad y b) un contrato entre el responsable del tratamiento originario y el destinatario de la información anonimizada.

De acuerdo con todo lo anterior, el problema que surge en relación con esta exigencia de la LOPD-GDD de anonimizar los datos de las denuncias (que no hayan sido investigadas) es que dicho proceso (como ha quedado detallado con anterioridad) implicaría, además de la obligación de adoptar ciertas garantías adicionales, que las entidades no puedan identificar quiénes son los interesados a los que pertenecen los datos incluidos en ellas. Ello podría conllevar que, en la práctica, algunas compañías no tengan suficiente información para poder demostrar el funcionamiento de sus modelos de prevención de la comisión de delitos, para poder hacer frente a posibles responsabilidades o para identificar denuncias que, *a priori* y de forma aislada, no tengan entidad suficiente como para que las entidades emprendan investigaciones o acciones, pero que, si se suceden de manera reiterada (en relación con un mismo sujeto o sobre un mismo tema), podrían ser calificadas de otra forma. En este sentido, si para poder alcanzar dichos fines no fuera suficiente con mantener un histórico de las denuncias anonimizadas, se debería valorar si —excepcionalmente— estas podrían ser conservadas fuera del entorno lógico del canal de forma seudonimizada[140], pero reforzando otras medidas, como por ejemplo las de seguridad (limitando los accesos) y confidencialidad, con el fin de minimizar los riesgos en materia de protección de datos.

En cualquier caso, las denuncias investigadas (archivadas o no), como, en su caso, las denuncias no tramitadas que excepcionalmente y de forma justificada se hayan conservado de forma seudonimizada con las precauciones expuestas anteriormente, podrían conservarse con los únicos fines de dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, dar cumplimiento a obligaciones legales o para poder hacer frente a acciones legales relacionadas con las materias que se pueden denunciar a través del canal de *whistleblowing*. La conservación de las denuncias no podrá realizarse de forma indefinida y, por ello, los responsables del tratamiento deberán fijar los plazos máximos de conservación de estas teniendo en cuenta los plazos de conservación de cierta documentación exigidos por la normativa (p. ej., la normativa de prevención de blanqueo de capitales exige que los documentos relacionados con esta materia sean conservados durante un periodo de diez años) y los plazos máximos de prescripción de las acciones legales relacionadas con las materias objeto de denuncia a través del canal.

f) Restricciones de autorizaciones de acceso a las denuncias

El acceso a los datos contenidos en estos sistemas debe quedar limitado exclusivamente a quienes, incardinados o no en el seno del responsable del tratamiento, desarrollen las funciones de control interno y de cumplimiento. No obstante, el artículo

137 AEPD: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, disponible en https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf).

138 AEPD: *Código de Buenas Prácticas en Protección de Datos para Proyectos de Big Data*, sección IV.4., pág. 30, disponible en https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf: "*Se deben* establecer medidas adicionales de seguridad en todos los elementos que intervienen en el proceso de la anonimización, como auditorías periódicas de las fuentes de información, de los canales de transmisión de la información, de las localizaciones físicas de las fuentes de información, etc*., aplicando los estándares, sellos y buenas prácticas en seguridad y privacidad de la información.* Este marco integral debería incluir un procedimiento de detección y notificación de posibles brechas de privacidad que pudieran surgir, como casos de re-identificación".

139 AEPD: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, sección 5, págs. 21 y 22.

140 La "seudonimización", de acuerdo con el artículo 4.5 del RGPD, es "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*".

24.2[141] de la LOPDGDD detalla que será lícito el acceso de otras personas (incluso por el personal de recursos humanos) cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales.

g) Limitación del derecho de acceso

La normativa de protección de datos, en los artículos 12 y ss. del RGPD, reconoce que los titulares de los datos tienen derecho a ejercitar una serie de derechos reconocidos y las compañías tienen la obligación de contestarles siempre (de forma positiva o negativa, según corresponda) en un plazo breve de tiempo (máximo de un mes). Entre dichos derechos cabe destacar, por su particularidad en el contexto de los sistemas de denuncias, el derecho de acceso de los afectados por una denuncia (*i. e.*, el denunciado, testigos y terceros). El derecho de acceso se regula en el artículo 15 del RGPD y da la opción de conocer, básicamente, qué categorías de datos se están tratando sobre dicho afectado, su procedencia, a quién han sido cedidos, con qué finalidades se están tratando y el plazo de conservación previsto. No obstante, este derecho, en el contexto del canal de denuncias, está limitado (art. 23 del RGPD) con el fin de preservar la confidencialidad sobre la identidad del denunciante, de acuerdo con la Directiva y el artículo 24.3 de la LOPDGDD sobre los datos del denunciante. Por lo tanto, ni la persona incriminada, ni los testigos ni los terceros que se vean afectados por una determinada denuncia podrán acceder a los datos del *whistleblower*. Además, el SEPD[142] y el CNIL[143] indican que no solo se debería proteger la identidad del denunciante ante los derechos de acceso, sino también la del denunciado y cualquier otro tercero. En este sentido, si el denunciado ejercita su derecho de acceso a una determinada denuncia, el responsable del tratamiento no solo debería eliminar los datos del denunciante, sino también los de, por ejemplo, los testigos.

h) Implementación de medidas de seguridad

El artículo 5.1.f del RGPD obliga a los responsables del tratamiento a implementar medidas técnicas y organizativas para garantizar la seguridad adecuada de los datos personales. En este sentido, el artículo 32 del RGPD exige que los responsables de los datos personales analicen el nivel de riesgo del tratamiento y, en consecuencia, implementen las medidas de seguridad que consideren apropiadas para dicho tratamiento. Dado que en los sistemas de *whistleblowing*, como se ha señalado con anterioridad, se tratan datos especialmente protegidos, las medidas de seguridad han de ser suficientemente sólidas como para impedir brechas de seguridad y accesos no autorizados al canal. Por lo tanto, después de realizar un análisis de los riesgos asociados al tratamiento, si en el canal de denuncias (por su ámbito) podrían incluirse datos, por ejemplo, de posibles comisiones de delitos, los responsables del tratamiento deberían llevar a cabo una evaluación de impacto[144] de acuerdo con lo señalado en el artículo 35 del RGPD.

2.4.2 · Impacto de la Directiva

La Directiva dedica un artículo específico, y algunas otras pautas a lo largo de su articulado, para regular cómo se deben tratar los datos personales que se incluyen o generan a través de estos canales por parte de las entidades privadas y organismos públicos. Con ello, la Directiva pretende garantizar —sobre todo— la protección de la identidad del denunciante y la protección de los datos de cada informante, cada denunciado y cada tercero al que se refiera la denuncia (por ejemplo, testigos o compañeros de trabajo relacionados con una determinada denuncia) en todas las fases del procedimiento de investigación.

Ciertamente, la Directiva no incluye obligaciones en materia de protección de datos de carácter nove-

141 El artículo 24.2 de la LOPDGDD señala que "*2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos*".

142 SEPD: *Directrices sobre Whistleblowing*; pág. 10: "*When access is granted to the personal information of any concerned individual, the personal information of third parties such as informants, whistleblowers or witnesses should be removed from the documents except in exceptional circumstances* [...]".

143 CNIL: *Guía del CNIL*, pág. 12: "*L'exercice de ce droit ne doit pas permettre à la personne qui l'exerce d'accéder aux données à caractère personnel relatives à d'autres personnes physiques*".

144 La AEPD ha publicado una guía práctica sobre cómo han de realizarse las evaluaciones de impacto, disponle en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

doso, ya que el artículo que la Directiva destina específicamente a esta materia se limita a recordar que los tratamientos de datos relacionados con los canales de denuncias se deben realizar cumpliendo con la normativa aplicable en materia de protección de datos. Sin perjuicio de ello, la Directiva sí enfatiza —mediante el traslado de obligaciones generales en materia de protección de datos al contexto de los canales de denuncias— algunos de los requisitos que deben cumplirse cuando se implementan dichos sistemas.

En este sentido, el artículo 17[145], en relación con el considerando 83 de la Directiva, establece que cualquier tratamiento de datos personales, incluido su intercambio o transmisión, deberá cumplir con las obligaciones establecidas por el RGPD y demás normativa aplicable, que, en el caso de España, es la LOPDGDD —en particular su artículo 24, tal y como se ha detallado con anterioridad—. El citado artículo 17 de la Directiva recuerda, además, el principio de minimización del dato, indicando que no se deben recopilar datos personales cuya pertinencia no resulte necesaria para tratar una denuncia específica y que, en el caso de que estos se recopilasen accidentalmente, se deberían eliminar sin dilación indebida.

La Directiva, además de su artículo 17, también reitera y aclara —en diversos preceptos— distintos principios y obligaciones en materia de protección de datos que han de ser aplicados en el contexto de los canales de denuncias. Sin perjuicio de ello, y como no podía ser de otra forma teniendo en cuenta el objeto de la Directiva, esta incide —con mayor anhelo— en que se respeten dichos requisitos cuando se traten los datos personales del denunciante.

Respecto al deber de información, el artículo 12.4.a)[146] de la Directiva obliga a que los interesados sean informados sobre la existencia de un canal de denuncias. Esta obligación ya viene impuesta de forma específica por el artículo 24.1 de la LOPDGDD (*vid.* epígrafe anterior) y, de forma supletoria, por los artículos 13 y 14 del RGPD y por el artículo 11 de la LOPDGDD, que obligan a que todo interesado sea informado sobre todo tratamiento relativo a sus datos personales. Además, la Directiva indica, en sus artículos 9.1.f[147] y 11.2.d[148] y en los considerandos 58 y 67, que deberá informarse al denunciante sobre las medidas previstas y adoptadas para tramitar la denuncia —no solo sobre la existencia del canal— en un plazo razonable y, como regla general, en el plazo de tres meses. Este plazo está en línea con el plazo máximo para tramitar una denuncia establecido por el artículo 24.4 de la LOPDGDD. No obstante lo anterior, hay que tener en cuenta que la Directiva (considerando 67 y art. 11.2.d) extiende dicho plazo de informar —al denunciante— sobre la tramitación de una denuncia (de tres meses) a seis meses, en circunstancias excepcionales por la posible complejidad de una denuncia. De ahí que, de manera extraordinaria, cuando se den supuestos especialmente complejos, se podría defender que el plazo para cumplir con el deber de información se puede extender a los seis meses.

En relación con el deber de confidencialidad, la Directiva destaca en diversos preceptos la obligación de mantener la confidencialidad de las denuncias. En particular, el artículo 16[149] en relación con

145 El art. 17 de la Directiva señala que "*Todo tratamiento de datos personales realizado en aplicación de la presente Directiva, incluido el intercambio o transmisión de datos personales por las autoridades competentes, se realizará de conformidad con el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680. Todo intercambio o transmisión de información por parte de las instituciones, órganos u organismos de la Unión se realizará de conformidad con el Reglamento (UE) 2018/1725. No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una denuncia específica o, si se recopilan por accidente, se eliminarán sin dilación indebida*".

146 El art. 12.4.a señala que "*Los Estados miembros velarán por que las autoridades competentes designen a los miembros del personal responsables de tratar denuncias, y en particular de: informar a cualquier persona interesada sobre los procedimientos de denuncia*".

147 El art. 9.2.f de la Directiva señala lo siguiente: "*Los procedimientos de denuncia interna y seguimiento a que se refiere el artículo 8 incluirán lo siguiente: un plazo razonable para dar respuesta, que no será superior a tres meses a partir del acuse de recibo o, si no se remitió un acuse de recibo al denunciante, a tres meses a partir del vencimiento del plazo de siete días después de hacerse la denuncia*".

148 El art. 11.2.d de la Directiva indica que "*Los Estados miembros velarán por que las autoridades competentes: den respuesta al denunciante en un plazo razonable, no superior a tres meses, o a seis meses en casos debidamente justificados*".

149 El art. 16 de la Directiva señala que "*Los Estados miembros velarán por que no se revele la identidad del denunciante sin su consentimiento expreso a ninguna persona que no sea un miembro autorizado del personal competente para recibir o seguir denuncias. Lo anterior también se aplicará a cualquier otra información de la que se pueda deducir directa o indirectamente la identidad del denunciante.*

2. Como excepción a lo dispuesto en el apartado 1, la identidad del denunciante y cualquier otra información prevista en el apartado 1 solo podrá revelarse cuando constituya una obligación necesaria y proporcionada impuesta por el Derecho de la Unión o nacional en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, en particular para salvaguardar el derecho de defensa de la persona afectada.

el considerando 82 de la Directiva prohíbe —como norma general— que se revele la identidad del denunciante. Ello reitera un principio ya plasmado en el artículo 24.3 de la LOPDGDD, que establece, en este mismo sentido, que se deben adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas (como, por ejemplo, los denunciados o los testigos) por la información suministrada, haciendo especial hincapié en la protección del denunciante.

Yendo un paso más allá, el considerando 84[150] de la Directiva advierte de que, en determinadas circunstancias, el derecho a la protección de datos debe ceder ante la protección que pretende instaurar la Directiva para preservar la identidad de los denunciantes y el buen fin de las investigaciones. Para fundamentar este criterio, dicho considerando hace referencia al artículo 23 del RGPD, que es el precepto que establece bajo qué circunstancias se podrían limitar los derechos de los interesados en materia de protección de datos, como por ejemplo el derecho de acceso o de información. En este sentido, la Directiva establece —de manera razonable—, por regla general, límites a derechos de protección de datos, por ejemplo del denunciado, para acceder a los datos de una denuncia o a ser informado sobre la identidad del denunciante.

En relación con los plazos de retención de las denuncias, la Directiva señala, en su artículo 18, que las denuncias se conservarán únicamente durante el período que sea necesario y proporcionado a efectos de cumplir con los requisitos impuestos por la Directiva u otras obligaciones impuestas por el Derecho de la Unión o de los Estados miembros. El artículo 24.4 de la LOPDGDD, tal y como se ha analizado previamente, concreta que las denuncias deberán ser suprimidas del canal de denuncias en un plazo de tres meses (con ciertas excepciones). De nuevo, hay que tener en cuenta que, sin perjuicio de ello, la Directiva (considerando 67 en relación con el art. 11.2.d) prevé que las investigaciones iniciales sobre las denuncias puedan extenderse excepcionalmente a un plazo de seis meses.

La Directiva también reconoce, en su artículo 18, el derecho a los denunciantes a comprobar, rectificar y aceptar las denuncias. Este artículo recuerda la existencia —en este caso para el denunciante— de los derechos en materia de protección de datos a acceder a los datos personales y a rectificarlos (arts. 15 y 16 del RGPD).

3 · CONCLUSIÓN

Aunque, sin duda, es pronto aún para valorar, en toda la extensión y con toda la exhaustividad que merece, la incidencia que esta Directiva puede tener en el establecimiento de un sistema integral de respeto a la legalidad y de lucha contra el fraude, la corrupción y las demás infracciones que entran dentro de su ámbito de aplicación material u objetivo, la Directiva constituye un auténtico "salto adelante" en el establecimiento de un verdadero sistema de prevención y de represión temprana de tales comportamiento o conductas irregulares.

Cabe esperar, en esta nueva legislatura que acaba de empezar, que el legislador español adopte medidas decididas para la efectiva y eficaz transposición de la Directiva a nuestro ordenamiento jurídico, que, si bien no completamente ajeno a la figura del "denunciante" (*whistleblower*) y a su protección jurídica, carece de una norma que regule tales cuestiones con un carácter integral y exhaustivo como el perseguido por la Directiva.

3. Las revelaciones hechas en virtud de la excepción prevista en el apartado 2 estará sujeta a salvaguardias adecuadas en virtud de las normas de la Unión y nacionales aplicables. En particular, se informará al denunciante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente informe al denunciante, le remitirá una explicación escrita de los motivos de la revelación de los datos confidenciales en cuestión [...]".

150 El considerando 84 de la Directiva señala que "*Los procedimientos establecidos en la presente Directiva y relacionados con el seguimiento de denuncias de infracciones del Derecho de la Unión en sus ámbitos de aplicación contribuyen a un objetivo importante de interés público general de la Unión y de los Estados miembros, en el sentido del artículo 23, apartado 1, letra e), del Reglamento (UE) 2016/679, ya que su objetivo es mejorar la ejecución del Derecho y las políticas de la Unión en determinados ámbitos en los cuales el incumplimiento puede provocar graves perjuicios para el interés público. Una protección efectiva de la confidencialidad de la identidad de los denunciantes resulta necesaria a fin de proteger los derechos y libertades de los demás, en particular los de los propios denunciantes, tal como establece el artículo 23, apartado 1, letra i), del Reglamento (UE) 2016/679. Los Estados miembros deben velar por que la presente Directiva sea eficaz, incluso, cuando sea necesario, restringiendo mediante medidas legislativas el ejercicio de determinados derechos de protección de datos de las personas afectadas en consonancia con el artículo 23, apartado 1, letras e) e i), y el artículo 23, apartado 2, del Reglamento (UE) 2016/679, en la medida y durante el tiempo que sea necesario a fin de evitar y abordar los intentos de obstaculizar las denuncias o de impedir, frustrar o ralentizar su seguimiento, en particular las investigaciones, o los intentos de averiguar la identidad del denunciante*".

4 · BIBLIOGRAFÍA

BACIGALUPO ZAPATER, Enrique: "Responsabilidad penal y administrativa de las personas jurídicas y programas de 'compliance' (a propósito del Proyecto de reformas del Código Penal de 2009)", *Diario La Ley*, n.º 7442, 9 de julio de 2010.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Informe de su Gabinete Jurídico n.º 195/2017*, disponible en https://www.aepd.es/es/documento/2017-0195.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, disponible en https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Código de Buenas Prácticas en Protección de Datos para Proyectos de Big Data*, disponible en https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Informe del gabinete jurídico n.º 0128/2007 sobre la creación de sistemas de denuncias internas en las empresas*.

BLÁZQUEZ AGUDO, Eva María: "Canal de denuncias o *Whistleblowing* en el ámbito laboral", en PUEBLA PINILLA, Ana de la y MERCADER UGUINA, Jesús (dirs.): *Tiempo de reformas. En busca de la competitividad empresarial y de la cohesión social*, Valencia: Tirant lo Blanch, 2019.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS: *Relatif aux traitements de donness a caractere personnel destines a la mise en oeuvre d'un dispositif d'alertes professionnelles*, 10 de diciembre de 2019, disponible online (solo en francés): https://www.cnil.fr/sites/default/files/atoms/files/referentiel-alertes-professionnelles_decembre-2019.pdf.

EUROPEAN COMMISSION. Directorate-General for Justice and Consumers: *Whistleblower protection. Fact sheet*. Abril 2018.

EUROPEAN COMMISSION. Directorate-General for Justice and Consumers: *Frequently Asked Questions*. 23 de abril de 2018.

Explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union Law ("*Exposición de motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión*").

Financial Incentives for Whistleblowers, informe de la *Financial Conduct Authority* y de la *Prudential Regulation Authority* del Reino Unido, de julio de 2014, disponible en https://www.fca.org.uk/publication/financial-incentives-for-*whistleblowers*.pdf.

GÓMEZ-JARA DÍEZ, Carlos: *Fundamentos modernos de la responsabilidad penal de las personas jurídicas. Bases teóricas, regulación internacional y nueva legislación española*, Buenos Aires, 2010.

GRUPO DE TRABAJO DEL ARTÍCULO 29: *Dictamen 1/2006 sobre la aplicación de las normas de la Unión Europea relativas a la protección de datos a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros*, Bruselas, 1 de febrero de 2006. Disponible *online* (en inglés) en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

GUAMÁN HERNÁNDEZ, Adoración: *La libertad de información del trabajador*, Valencia: Tirant lo Blanch, 2005.

KAFTERANIS, Dimitrios: "Rethinking financial rewards for whistle-blowers under the proposal for a Directive on the protection of whistle-blowers reporting breaches of EU law", *Nordic Journal of European Law*, vol. 2. n.º 1, 2019.

KOHN, Stephen: *The new whistleblower's handbook: a step-by-step guide to doing what's right and protecting yourself*, Globe Pequot, Guiltord, Connecticut, 2017. https://www.zuckermanlaw.com/sp_faq/what-is-a-whistleblower-reward/.

LÓPEZ BAELO, Raúl: "*Whistleblowing* y relaciones laborales: informantes, garantías y mecanismos de denuncia", artículo ganador del premio de jóvenes laboralistas FORELAB 2019. Disponible en https://www.andersentaxlegal.es/recursos/doc/portal/2019/01/09/directiva-del-parlamento-europeo-y-del-consejo.pdf.

LÓPEZ CUMBRE, Lourdes: "Protección para los trabajadores denunciantes (*whistleblowers*)", *Análisis GA_P*. Diciembre 2019. Disponible en https://www.ga-p.com/wp-content/uploads/2019/12/Protección-para-los-trabajadores-denunciantes-whistleblowers.-1.pdf

LOUSADA AROCHENA, José Fernando: "Sistemas de denuncias internas (*Whistleblowing*) y derechos fundamentales en el trabajo", *Trabajo y Derecho*, n.º 52, 2019.

LOZANO CUTANDA, Blanca: "La directiva de protección del denunciante", *Diario La Ley*, n.º 9550, Sección Tribuna, 10 de enero de 2020.

MARTÍNEZ SALDAÑA, David y MORENO LUCENILLA, Ignacio: "La Protección del *whistleblower* y el *compliance* laboral", *Revista de Información Laboral*, n.º 12, 2018.

MARTÍNEZ SALDAÑA, David: "El Tribunal Constitucional otorga el amparo a un "proto-whistleblower" (la STC 146/2019, de 25 de noviembre, como contrapunto a la STC 126/2003, de 30 de junio)", *El Foro de Labos*. Disponible en https://forodelabos.blogspot.com/2020/01/el-tribunal-constitucional-otorga-el.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+ElForoDeLabos+%28El+Foro+de+Labos%29.

MERCADÉ PIQUERAS, Christel: "El canal de denuncias internas (*Whistleblowing*): La perspectiva laboral, investigación, garantías y deber de protección de datos", ponencia impartida en el marco del XX Congreso de ASNALA. Segovia, 26 de octubre de 2019.

MERCADER UGUINA, JESÚS R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Madrid: Francis Lefebvre, 26 de abril de 2019 (3.ª edición).

MORALES PRATS, Fermín: "La responsabilidad penal de las personas jurídicas (arts. 31 bis., supresión, 33.7, 66 bis., 12, 130.2 CP)", en Quintero Olivares, Gonzalo (dir.): *La reforma penal de 2010: análisis y comentarios*, Aranzadi, 2010.

NIETO MARTÍN, Adán: "Investigaciones internas, *whistleblowing* y cooperación: la lucha por la información en el proceso penal", *Diario La Ley*, n.º 8120, 5 de julio de 2013.

NIETO ROJAS, Patricia: "*Whistleblowers*. Aspectos laborales de la Directiva relativa a la protección de las personas que informen sobre infracciones de Derecho de la UE", *El Foro de Labos*. Disponible en https://forodelabos.blogspot.com/2019/10/whistleblowers-aspectos-laborales-de-la.html

PÉREZ TRIVIÑO, José Luis: "*Whistleblowing*", *Eunomía. Revista en Cultura de la Legalidad*, n.º 14, abril-septiembre 2018. Disponible en https://e-revistas.uc3m.es/index.php/EUNOM/article/view/4170/2694.

Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union Law ("*Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión*"). Brussels, 23.4.2018. COM (2018) 218 final. 2018/0106 (COD).

PUEBLA PINILLA, Ana de la: "Impacto laboral de la ley de secretos empresariales", en PUEBLA PINILLA, Ana de la y MERCADER UGUINA, Jesús (dirs.): *Tiempo de reformas. En busca de la competitividad empresarial y de la cohesión social*, Valencia: Tirant lo Blanch, 2019.

RAGUÉS I VALLÉS, Ramón: *Whistleblowing. Una aproximación al Derecho penal*, Madrid: Marcial Pons, 2013.

REY GUANTER, Salvador del: *Libertad de expresión e información y contrato de trabajo*, Madrid: Civitas, Madrid, 1994.

RODRÍGUEZ-MOURULLO, Gonzalo: "La responsabilidad penal de las personas jurídicas y los principios básicos del sistema", *Abogados*, 2010.

RODRÍGUEZ YAGÜE, Cristina: "La protección de los Whistleblowers en el ordenamiento español", en ARROYO ZAPATERO, Luis y NIETO MARTÍN, Adán (coords.): *Fraude y corrupción en el Derecho penal económico europeo. Eurodelitos de corrupción y fraude*, Cuenca: Ediciones de la Universidad de Castilla-La Mancha, 2006.

ROJO TORRECILLA, Eduardo: "La protección del derecho constitucional a la libertad de expresión en el ámbito de las relaciones de trabajo. Notas a la sentencia del TC núm. 146/2019, de 25 de noviembre". Disponible en http://www.eduardorojotorrecilla.es/2019/12/la-proteccion-del-derecho.html.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 30 de julio de 2002.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS PERSONALES: *Guidelines on processing personal information within a whistleblowing procedure*, publicadas el mes de julio de 2016 y actualizadas en diciembre de 2019. Disponible en https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en.

TODOLÍ SIGNES, Adrián: "La regulación de los *whistleblowers*", *Agenda Pública*, *El País*, 12 de septiembre de 2015. Disponible en http://agendapublica.elpais.com/la-regulacion-de-los-whistleblowers/.

Whisteblower reward programmes, de 27 de septiembre de 2018. Disponible en https://knowledgehub.transparency.org/assets/uploads/helpdesk/Whistleblower-Reward-Programmes-2018.pdf.

ZUCKERMAN, Jason y STOCK, Matthew: *What is a whistleblower reward?* Disponible en https://www.zuckermanlaw.com/sp_faq/what-is-a-whistleblower-reward/.