Sistema de denuncias y protección de datos personales

Breaches procedures and data protection

ROSARIO CRISTÓBAL RONCERO*

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantías de los Derechos digitales (en adelante, LOPD) se dicta para adaptar el ordenamiento jurídico español al Reglamento UE 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril, 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)[1].

Esta Ley, además de regular los derechos a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), a la desconexión digital en el ámbito laboral (art. 88), a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89), a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90) y los derechos digitales en la negociación colectivo, introduce un sistema de información de denuncias internas, a cuyo tenor se establece una especial protección para los denunciantes que también va a desplegar efectos en el ámbito laboral. Estos sistemas de recepción y conocimiento de infracciones se encuadran bajo las exigencias de la legislación aplicable en materia de protección de datos, siempre que traten denuncias referidas a normas, fundamentos o principios, cuyo incumplimiento tenga consecuencias efectivas sobre la pervivencia de la relación contractual entre la empresa y el denunciado.

El art. 24 LOPD regula un sistema de denuncias internas desde la perspectiva del derecho de protección de datos personales, referido a los límites de acceso a los datos de las personas, la confidencialidad del tratamiento o la limitación temporal en orden a la conservación de las denuncias.

Recientemente, se ha regulado la protección a los denunciantes (*whistelblowing)* en el ámbito de la Unión Europea. En efecto, la Directiva UE2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, relativa a la protección de las personas que informan sobre infracciones del Derecho de la Unión (en adelante, DPII) configura, de forma profusa, un sistema de canales de denuncia, externo e interno, que protege la confidencialidad, el anonimato y la no represalia del denunciante[2]. La Directiva entró en vigor el pasado 17 de diciembre, si bien el plazo de

* Profª Titular de Derecho del Trabajo y de la Seguridad Social. Universidad Complutense de Madrid.

[1] DOUE núm. 119, de 4 de mayo de 2016.

[2] Siguiendo las Resoluciones del Parlamento Europeo de 20 de enero sobre la Función de los denunciantes en la protección de los intereses financieros de la Unión y la de 24 de octubre de 2017 sobre Medidas legítimas para la protección de los denunciantes de infracciones que actúan en aras del interés público, en abril de 2018 la Comisión europea presentó la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del Derecho, que llevan después a la aprobación de la Presente Directiva.

trasposición a nuestro Ordenamiento concluye el 17 de diciembre de 2021. Por tanto, los Estados Miembros disponen de dos años para adaptar, con amplio margen, sus legislaciones internas al contenido mínimo previsto por la Directiva.

Estamos, pues, ante una norma esperada, un elemento más en el engranaje normativo que el legislador comunitario –pero también, el nacional– propone para articular la obligación de establecer canales de denuncia y a su vez medidas que garanticen la protección de los denunciantes. La principal virtualidad de la Directiva es que, con su sola existencia, despeja los debates sobre los cauces del sistema de denuncia, aportando luz en un contexto absolutamente necesitado de seguridad jurídica. Se busca, en definitiva, reforzar la protección del *whistelblower* y el ejercicio del derecho a la libertad de expresión e información reconocido en al art. 10 CEDH y en el art. 11 de la Carta de los Derechos Fundamentales y con ello se aspira a incrementar su actuación "en el descubrimiento de prácticas ilícitas o delictivas que tengan un impacto en el derecho de la Unión Europeo, sus políticas o presupuesto"[3].

En conclusión, esta Directiva contribuye a una mejor implementación del Derecho de la Unión Europea con un alcance muy amplio en el ámbito del *compliance*, si bien nosotros abordaremos de forma específica las medidas de protección del informante en el ámbito laboral.

1. ÁMBITO DE PROTECCIÓN

El Capítulo I recoge las reglas de configuración sobre el alcance material y el ámbito personal de los "denunciantes" que informan sobre infracciones del Derecho de la Unión.

Asimismo, en este Capítulo se disponen las definiciones que se ofrecen en el marco de esta Directiva, en aras de determinar y garantizar la protección de los sujetos con ocasión de su actuación en el marco del *whistleblowing*. Muchas de estas definiciones son nuevas y algunas desconocidas para nuestro ordenamiento jurídico laboral. Sin duda, debe agradecerse la voluntad del legislador europeo por facilitarnos luz para entender el ámbito de aplicación y protección de los informantes y, sobre todo, el alcance de sus garantías en el ejercicio y desarrollo de las relaciones laborales.

1.1. Ámbito de aplicación material

El art. 2 de la Directiva establece y define el ámbito de aplicación material a través de la delimitación de las infracciones. Así, se consideran infracciones del Derecho de la Unión "las acciones u omisiones que sean ilícitas y que estén relacionadas con los ámbitos de actuación de la Unión o que desvirtúen su objeto o finalidad"[4]. En concreto, se precisan los siguientes: contratación pública; servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo; seguridad de los productos; seguridad del transporte; protección del medio ambiente; protección contra las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, salud animal y bienestar de los animales; salud pública; protección de los consumidores; y protección de la intimidad y los datos personales, y seguridad de las redes y los sistemas de información [art. 2.1 a) Directiva].

[3] L. Bachmaier Winter: "*Whistelblowing* europeo y compliance: la Directiva EU de 2019 relativa a la protección de las personas que reporten infracciones del Derecho de la Unión", *Diario La Ley*, núm. 9527, 2019, p. 3.

[4] El ámbito de la Directiva también se extiende a infracciones que afecten a los intereses financieros de la Unión, tal y como se definen en el artículo 325 del Tratado y tal y como se concretan en la correspondientes medidas de la Unión; e infracciones relativas al mercado interior (art. 26.2. TFUE), incluidas las infracciones de las normas en materia de competencia y ayudas estatales; y también en relación con actos que infrinjan las normas del impuesto sobre sociedades o con disposiciones cuya finalidad deba obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades [art. 2.1 a) Directiva].

Además, la Directiva se extiende a "todos aquellos ámbito no regulados en el marco de instrumentos sectoriales específicos que deben ser completados por la presente Directiva, de tal modo que sean conformes con las normas mínimas previstas en ellas" (Considerando 20). En este sentido, cabe plantearse si dentro del ámbito de la Directiva quedaría protegido la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual y el acoso por razón de sexo" [art. 4.2 e) ET]. Como tendremos oportunidad de analizar, las represalias, por el hecho de la denuncia, se deben considerar como vulneración de un derecho fundamental. En este contexto, el acoso en sus distintas formas ocupa un lugar preferente de protección, sobre todo, cuando el trabajador se sienta discriminado, vejado o acosado por el empresario, por sus superiores, por otros trabajadores o por terceros, como consecuencia de la denuncia de irregularidades o por la denuncia del propio acoso[5].

El ámbito de aplicación de la Directiva no afecta, sin embargo, al ejercicio de los derechos de los trabajadores a consultar a sus representantes o sindicatos, ni a las medidas perjudiciales injustificadas derivadas de tales consultas ni a la autonomía de los interlocutores sociales a celebrar convenios colectivos (art. 3.4 DPII)[6].

1.2. Ámbito de aplicación personal

Uno de los aspectos más complicados que presenta la Directiva por la extensión de su alcance subjetivo, es el que tiene que ver con la determinación y concreción del ámbito de aplicación personal.

En efecto, se protege no sólo a los denunciantes del sector público sino también a los del sector privado, que comuniquen o revelen públicamente información sobre infracciones del Derecho de la Unión, que se hayan conocido en un contexto laboral, siempre que tuvieran motivos razonables para creer que la revelación era veraz en el momento de la denuncia[7]. En este sentido, se precisa que se aplicará, como mínimo a:

– las personas que tengan la condición de trabajadores en el sentido del artículo 45. 1 TFUE. Respecto del concepto comunitario de trabajador, hay que subrayar, en consonancia con la jurisprudencia del TJUE, que se incluye a los trabajadores por cuenta ajena en el sentido del art. 1.1 ET, ya sean a trabajadores con contrato indefinido, temporal, a tiempo completo o a tiempo parcial, pero también se consideran incluidas dentro del concepto de trabajador las relaciones laborales atípicas mediante la técnica de las relaciones laborales especiales, así como los funcionarios, empleados del servicio público y cualquier otra personas que trabaje en el sector público[8].

[5] En el derecho alemán esta garantía viene, específicamente, establecida en el § 16. 1 de la *Allgemeines Gleichbehandlungsgesetz*, AGG, Ley alemana de Igualdad de trato, que prevé una "garantía de indemnidad en sentido estricto que sanciona con nulidad por discriminatorio las represalias frente a las quejas de todo tipo formuladas en relación con el principio de igualdad de trato", en R. CRISTÓBAL RONCERO: Igualdad de mujeres y hombres: Un estudio de Derecho comparado", *REDT* 2010, núm. 147, p. 548. En nuestro país, el art. 48 de la Ley 2/2007 para la Igualdad efectiva de mujeres y hombres " obliga a las empresas a arbitrar procedimientos específicos para la prevención del acoso sexual y por razón de sexo y para dar cauce a la denuncias o reclamaciones que puedan formular quienes hayan sido objeto del mismo".

[6] Ni tampoco a la protección del secreto médico y del secreto profesional en la relación cliente-abogado, el secreto de las deliberaciones judiciales y las normas sobre protección y confidencialidad establecidas a nivel nacional en la ley de enjuiciamiento criminal (art. 3.3 DPII)

[7] Este requisito se construye sobre un triple presupuesto: 1.-Salvaguarda 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; 2.– El denunciante que comunique informaciones inexactas sobre infracciones por error cometidos de buena fe no queda exento de protección; 3.– Irrelevancia de los motivos de los denunciantes al denunciar, en todo caso deben gozar de protección (considerando 32).

[8] En efecto, el concepto de trabajador en el ámbito del Derecho de la Unión Europea se apoya en la *vis attractiva* del Derecho del Trabajo que alcanza a los funcionarios "laboralizando su relación", en A. MONTOYA MELGAR: *Tendencias actuales del Derecho del Trabajo*, Ed. CEU, 2014, pág. 7.

– las personas que tengan la condición de trabajadores no asalariados, en el sentido del artículo 49 del TFUE; se incluye a los autónomos, voluntarios, trabajadores en prácticas sin remuneración, proveedores de servicios y "facilitadores" y personas relacionadas con los denunciantes que puedan sufrir represalias en un contexto laboral y las entidades jurídicas que sean propiedad del denunciante paras las que trabaje o mantenga cualquier otro tipo de relación laboral que asisten al denunciante.

– los accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

Además, el ámbito de aplicación y protección de la Directiva se extiende a sujetos que no entran dentro de la categoría de trabajador. Alcanza a denunciantes que comunican o revelan información sobre infracciones obtenidas en el marco de una relación laboral extinguida, así como también al informante que denuncia infracciones obtenidas durante el proceso de selección de negociación precontractual. En definitiva, se aplica a trabajadores cuyo contrato de trabajo se ha extinguido o todavía no ha comenzado (art. 4 DPII).

Con ello, el legislador europeo otorga protección jurídica a todos aquellos que puedan ser objeto de represalias en el ámbito de las relaciones laborales *stricto sensu* o en el ámbito de la función pública, extendiéndose, además, a la protección a terceros personas jurídicas, físicas, como: familiares, compañeros de trabajad y "facilitadores", que por su vinculación con el denunciante pueden ser objeto de represalias (art. 4 DPII).

Por lo que se refiere a la protección y apoyo a los informantes, aquélla se vinculó, en un principio, a la actuación de buena fe del denunciante. Recuérdese que, a los efectos de la Directiva, el denunciante es "una persona física que comunica o revela públicamente información sobre infracciones obtenidas en el contexto de sus actividades laborales".

En la práctica resulta difícil deslindar si la denuncia está motivada por un interés público o personal. De hecho, la Directiva 2019/1937 elimina el requisito de la buena fe en la protección a los *whistleblowers*, de forma que las medidas de protección se aplican a los denunciantes que "tengan motivos fundados para pensar que la información notificada es veraz en el momento de la denuncia y que es susceptible de protección. Por tanto, las razones que llevan al informante a canalizar una denuncia se tornan irrelevantes, "siempre que los hechos denunciados sean ciertos o el denunciante estuviera en la creencia razonable de que lo eran"[9].

En definitiva, la Directiva amplía las garantías a una serie sujetos, con mayor o menor vinculación en el contexto laboral, para asentar las bases mínimas de protección a todos los concernidos y afectados por la información de infracciones del Derecho de la Unión.

2. CANALES DE DENUNCIA

La obligación de establecer canales de denuncia constituye uno de los pilares fundamentales sobre los que se asienta el espíritu de la Directiva sobre protección de las personas que informen infracciones del Derecho de la Unión Europea. En primer lugar, se establece el canal de denuncia interna, es decir, se invita a los informantes para que acudan a este medio como vía preferente para tratar la infracción dentro de la organización y sin riesgo a represalias; y en segundo lugar, se propone, el sistema de denuncia externas, como mecanismo subsidiario que persigue idénticos objetivos y garantías, si bien con posible repercusión *ad extram* de lo acontecido en la empresa. Es relevante advertir, no obstante, que no existe deber de denuncia, pero sí se obliga a la creación e implantación de estos cauces y a que se confiera, en todo caso, protección al denunciante.

[9] J.R. MERCADER UGUINA: *Protección de datos en la relaciones laborales*, Ed. Francis Lefebvre, Madrid, 2018, p. 165.

Como principio general para la detección y prevención de infracciones del Derecho de la Unión Europea se pretende que la información pertinente llegue de manera rápida a quienes están más próximos a la fuente del problema y tienen más posibilidades de investigarlo y competencias para remediarlo.

El art. 24 LOPD regula también los sistemas de denuncias –aunque en nuestro ordenamiento jurídico sólo se refiere a los internos– para conocer la realización de posibles irregularidades dentro de la empresa no sólo desde la perspectiva de la protección de datos, pues alcanza también a las medidas que se adopten para garantizar y salvaguardar dicha protección. En efecto, estos canales permiten que la organización empresarial o a la entidad pública actúe e intervenga con un doble objetivo: por un lado, conocer de forma inmediata las infracciones cometidas, y por otro, para detectar los fallos en la prevención y reaccionar con celeridad frente a las irregularidades e infracciones.

Las entidades jurídicas de los sectores públicos y privados tienen potestad para implantar la creación y seguimiento de canales de denuncias internos (art. 8 DPI).

Mientras que la Directiva comunitaria dispone la obligación de instaurar estos sistemas en las empresas privadas que tenga 50 empleados o más y en todas las entidades públicas con la salvedad de exención a los municipios "pequeños" –menos de 10.000 habitantes– y entidades con menos de 50 empleados, el art. 24 LOPD se limita a disponer su licitud sin establecer una obligación específica de organizar e incorporar estos canales ni en el ámbito privado (art. 24.1) ni en las Administración públicas (art. 24.5)[10]. En este sentido, nuestro ordenamiento jurídico tendrá que adoptar las medidas necesarias para garantizar la obligatoriedad de imposición de los sistemas de denuncia en uno y en otro caso. Para ello, habrá que imponer a los empresarios la obligación de implantar canales de denuncia objetivos y fiables, de forma que "la información recogida y tratada se trasmita solo a las personas responsables de la investigación" y, en todo caso, se garantice la adopción de las medidas necesarias para realizar el seguimiento e investigación de los hechos denunciados[11].

La directiva regula tres tipos de canales de denuncia de infracciones: 1) internos, dentro de una entidad jurídica pública o privada, 2) externos, dependientes de las autoridades competentes que designen los Estados miembros y 3) la revelación pública, consistente en la puesta a disposición del público de información sobre infracciones.

1.– Canales de denuncia internos en una entidad jurídica pública o privada

Los canales de denuncia internos deben implantarse previa consulta con los interlocutores sociales, cuando así lo establezca el derecho nacional (art. 8 DPII). Nada dice el art. 24 LOPD a este respecto, pero cabe augurar su necesaria participación en el diseño y configuración de estos sistemas.

En efecto, entre las competencias que el legislador estatutario otorga a la representación de los trabajadores en la empresa se encuentra la de su intervención en los procesos de consulta y negociación. Una posible opción es que se configure y se organice el canal de denuncias mediante negociación colectiva o acuerdo de empresa o, en su defecto, a través

[10] Se impone una obligación de mínimos. Por tanto, la Ley que transponga el contenido de la Directiva podrá impulsar o directamente establecer la obligación de creación de estos sistemas de denuncias e incluso extenderlo, a empresas de menor tamaño estableciendo requisitos menos exigentes que la propia Directiva, pero "siempre garantizando la confidencialidad y el seguimiento diligente de la denuncia" (considerando 49)

[11] En cierto, modo el párrafo 4º del art. 23 LOPD ya precisa que se deben adoptar 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.

de la decisión del empresario previa consulta con los representantes legales en la empresa.

Para conseguir su eficacia real, la consulta debería permitir a los representantes de los trabajadores sobre la base de la información recibida reunirse con el empresario, contrastar sus puntos de vista y opiniones con objeto de poder llegar a un acuerdo sobre la implantación y configuración de los canales de denuncia.

En todo caso, su actuación se debe garantizar conforme al deber de buena fe con vistas a la consecución de un acuerdo y al de de confidencialidad en relación con la información que, en legítimo interés de la empresa, del centro de trabajo o de los informantes les haya sido expresamente comunicada con carácter reservado. En este sentido, se ha pronunciado el Tribunal Constitucional, en su sentencia de 11 de noviembre de 2002[12], al declarar que ningún tipo de documento entregado por la empresa al Comité podrá ser utilizado ni fuera del ámbito estricto de aquélla ni tampoco para fines distintos de los que motivaron su entrega. Y, añade el Alto Tribunal, que tal obligación "subsistirá incluso tras la expiración del mandato e independientemente del lugar en que se encuentren de conformidad con lo establecido en el art. 65.2 y 65.3 ET"[13].

Ahora bien, este deber de sigilo debe cohonestarse con la obligación de la representación legal de los trabajadores de informar a sus representados en todos los temas y cuestiones señalados en el art. 64.7.e) ET en cuanto directa o indirectamente tengan o puedan tener repercusión en las relaciones laborales[14], tal y como señala el texto de la propia Directiva.

Un aspecto relevante de la Directiva 2019/1037 es que, además de obligar a que se establezcan procedimientos internos de denuncia, exige la consignación de un contenido mínimo en estos canales de denuncia. En efecto, se establecen unas exigencias mínimas que deben cumplir todos los Estados miembros[15] y que, en cierta medida, favorecen la eficacia de este sistema de protección de las personas que informen sobre derechos de la Unión Europea. En este sentido, se han propuesto como posibles requisitos, entre otros: "el apoyo por parte de la dirección; la información previa a los destinatarios del mecanismo, la accesibilidad, proporcionalidad y documentación del sistema, la independencia del órgano de gestión, sistema de infracciones y sanciones y la protección del denunciante o informador"[16]. En concreto, la Directiva establece que deberán incluir, al menos, las siguientes exigencias:

a) Confidencialidad.– Los canales para recibir denuncias deben estar diseñados y gestionados de forma que se garantice, en todo caso, la confidencialidad de la identidad del denunciante y/o de cualquier tercero que se mencione en la denuncia. En este sentido, el deber de confidencialidad debe alcanzar también a los no afectados, de forma

[12] STC 213/2002 (RTC 2002, 213)

[13] Sin embargo, la empresa no estará obligada, si bien de manera excepcional, a comunicar aquellas informaciones específicas relacionadas con secretos industriales, financieros o comerciales cuya divulgación pudiera, según criterios objetivos (STS 13-02-1989 y STSJ Castilla La Mancha 24-11-2005, rec. 1588/05), obstaculizar el funcionamiento de la empresa o del centro de trabajo u ocasionar graves perjuicios en su estabilidad económica, aunque la excepción mencionada no abarca aquellos datos que tengan relación con el volumen de empleo en la empresa (art. 65.4 ET). Por consiguiente, cuando la representación legal de los trabajadores acredite la pertinencia de la documentación complementaria, la empresa solo podrá negarse a su aportación, cuando concurran las circunstancias mencionadas, cuya prueba le corresponderá, de conformidad con lo dispuesto en el art. 217.3 LEC, salvo que se trate de datos relacionados con el volumen de empleo de la empresa. La negativa infundada a aportar documentación pertinente constituye falta grave, de conformidad con lo dispuesto en el art. 7.7 RDL 5/2000, aunque podría llegar a calificarse como falta muy grave (art. 8.3 RDL 5/2000), de acreditarse, que dicha decisión empresarial impidió que el período de consultas alcanzase sus fines (STC 213/2002).

[14] STSJ Murcia 23-07-2001, rec.617/01, resol. 1107/01. En: https://app.vlex.com/#vid/17456032.

[15] Lo que contribuirá a un mayor alcance de las denuncias y a una esperada uniformidad de sistemas dentro de la UE.

[16] J.F. Lousada Arochena: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *Trabajo y Derecho,* núm. 52, 2019, pág.3.

que su acceso a la información sea del todo imposible al tratarse de personal "no autorizado".

b) Comunicación escrita.– Se debe comunicar al denunciante, por escrito y con acuse de recibo, la recepción de la denuncia en un plazo de siete días.

c) Información, clara y fácil, sobre los procedimiento de denuncias a los posibles denunciantes que deben incluir no solo la existencia y/o conocimiento de esta vía de actuación, sino también las forma y procedimiento de acceso y utilización.

d) Órgano de gestión y seguimiento de la denuncia.– Para el desempeño de estas funciones se puede designar a un tercero externo o a un departamento, nombrado a tal efecto por la empresa, para entender de cuantas cuestiones les sean atribuidas. En principio, tienen señaladas competencias "ordinarias" o "simples", como son: la recepción de la denuncia, la comunicación con el denunciante, la solicitud de información adicional, y en todo caso, la contestación de la denuncia, que debe realizarse en un plazo razonable. A estos efectos, se distinguen dos plazos diferentes en función de si ha habido acuse de recibo o no. En caso afirmativo, la contestación no podrá ser "superior a tres meses a partir del acuse de recibo", y si éste no se remitió, será también "de tres meses, pero a partir del vencimiento del plazo de siete días después de hacerse la denuncia".

Además, el sistema de denuncias, consecuencia del carácter de confidencialidad del que se le ha dotado, ha dado origen a una modalidad especial de competencia, que puede llamarse "competencia reforzada", en virtud de la cual a la persona o departamento designados se les exige, además, un seguimiento diligente de la denuncia, incluso anónima, cuando así lo establezca el Derecho nacional.

La Directiva, al igual que sucede durante el seguimiento de la denuncia reforzada y diligente, deja a la discrecionalidad de los Estados miembros la aceptación o no de denuncias anónimas (art. 5.2. DPII). En todo caso, podrán presentarse por escrito en formato electrónico o en papel o de palabra, por vía telefónica, grabadas o no grabadas, o en reuniones presenciales con la personas o departamento designados para gestionar y seguir la denuncia, cuando así lo solicite el informante (art. 9.2 DPII).

En relación con la aceptación denuncias anónimas, el art. 24 LOPD acepta la licitud de canales que aceptan y tramitan denuncias en las que se desconoce la identidad del informante. Por tanto, se garantiza el anonimato del denunciante sin que esta previsión legal quede exenta de problemas jurídicos detectados por la doctrina científica y por la práctica judicial.

2.– Canales de denuncia externos, dependientes de las autoridades competentes que designen los Estados miembros

Aunque se incentiva el uso de canales internos, es también posible presentar la denuncia a través de un sistema externo. Varias son las razones que se encargan de establecer precisiones sobre la posibilidad de optar por este canal. En primer lugar, la ausencia de implantación de un sistema interno de denuncias en la empresa o en la institución pública. En segundo lugar, la falta o insuficiencia de funcionamiento apropiado del sistema interno de la organización. En tercer lugar, las deficiencias en el desarrollo del procedimiento por inobservancia de los requisitos formales– por ejemplo, diligencia debida el seguimiento, adopción de medidas en el plazo establecido– y en fin, porque exista verdadero temor a represalia, al no poder esperar razonablemente que los canales internos funcionen de forma adecuada.

El capítulo III de la Directiva 2019/1937 (arts. 10-14 DPII) se ocupa de la regulación de los canales externos; exige, en todo caso, que sean independientes y autónomos, y garanti-

cen la exhaustividad, integridad y confidencialidad de la información (art. 12 DPII).

Al igual que sucede con los canales de denuncia internos, la Directiva incluye un contenido mínimo para el adecuado funcionamiento del sistema y, además, requiere que el personal que los gestione tenga formación específica. Por lo demás, las exigencias mínimas que deben reunir los procedimientos de denuncias externas son muy similares a las exigidas para los procedimientos externos: confidencialidad; comunicación escrita; información, clara y fácil; y designación de órganos de gestión y seguimiento de la denuncia.

Sin perjuicio de las razones que favorecen la opción de los canales de denuncia internos frente a los externos, el recurso a los procedimientos de denuncia externos no quedan supeditados al requisito previo de haber acudido, con anterioridad, a los canales internos, por lo que el denunciante podrá escoger si utiliza los cauces internos o formula la denuncia directamente ante un órgano externo (art. 10 DPII)

Como regla general, a la empresa le interesará que se acuda a los canales de denuncia internos y evitar las denuncias externas "por temor al riesgo reputacional". En este sentido, la Directiva también muestra preferencia por que se recurra, cuando sea posible y adecuado, a los canales internos con el fin de contribuir a fomentar la cultura de buena gobernanza y responsabilidad social. En efecto, la Directiva señala que "debe animarse a los denunciantes a utilizar en primer lugar los cauces internos e informar a su empleador (…), en particular, cuando piensen que la infracción puede resolverse de manera efectiva dentro de la organización, y siempre que el denunciante considere que el cauce interno no presenta riesgo de represalias"[17].

Ahora bien, esto no significa que el denunciante deba valorar en cada supuesto el riesgo de represalias para decidir si acude directamente a la vía externa o a los cauces de denuncia internos; ni tampoco cabe deducir que si acude directamente al cauce externo, esta decisión deba incidir en las medidas de protección que se le han de garantizar en todo caso[18]. Por tanto, el informante es libre de optar por una vía u otra. No obstante, el legislador le recuerda la buena práctica empresarial y sobre todo, la preferencia de opción por el canal interno si la infracción puede ser resuelta a través de esta vía (art. 7.1 DPII)

3.– La revelación pública

La revelación pública constituye la tercera vía de denuncia que dispone la Directiva 2019/1937. Está regulada en el Capítulo IV, en concreto, en el art. 15. Consiste en la puesta a disposición del público de información sobre infracciones. Cierto es que este supuesto puede quedar más alejado del ámbito de las relaciones laborales en la empresa privada no así de la instituciones públicas; de hecho, constituye un canal adicional de protección de las personas que informe sobre infracciones del Derecho de la Unión Europea.

Se puede acudir a la revelación pública, cuando se haya denunciado primero por canales internos o externos y la "persona informante" tenga motivos razonables para pensar:

- Que no se hayan tomado medidas al respecto en el plazo previsto para la contestación
- Que la infracción constituye un peligro inminente o manifiesto para el interés público, por ejemplo: situación de emergencia o riesgo de daños irreversibles.
- Que exista, en caso de denuncia externa, un riesgo de represalias o haya pocas probabilidades de que

[17] Considerando 47 Directiva 2019/1937.

[18] L. Bachmaier Winter: "Whistelblowing europeo y compliance: la Directiva EU de 2019 relativa a la protección de las personas que reporten infracciones del Derecho de la Unión", *cit.*, p. 9.

se dé un tratamiento efectivo a las circunstancias particulares del caso. Por ejemplo, que puedan ocultarse o destruirse las pruebas o que una autoridad esté en connivencia con el autor de la infracción o implicada en la infracción.

Este procedimiento no será de aplicación cuando una persona revele información directamente a la prensa con arreglo a las disposiciones nacionales específicas por las que establezca un sistema de protección relativo a la libertad de expresión e información.

3. PROTECCIÓN AL TRABAJADOR QUE DENUNCIA INFRACCIONES O IRREGULARIDADES EN EL ÁMBITO DE TRABAJO

Antes de que se apliquen las medidas de protección frente a posibles desagravios del trabajador por haber informado de determinadas irregularidades en el seno de la empresa o de la administración pública, el denunciante está obligado a creer en la veracidad de los hechos que denuncia y a proceder a la denuncia a través de los cauces previstos para ello (canal interno o externo, principalmente). El resultado positivo de estas comprobaciones acredita el cumplimiento del procedimiento de información por parte del denunciante, lo que permite que se activen las medidas de protección para prohibir todo tipo de represalias.

La principal medida de protección es la confidencialidad de la identidad del informante, salvo que exista consentimiento expreso por su parte (art. 16.1.DPII) o que la revelación de su identidad constituya una obligación necesaria y proporcionada en el marco de un proceso judicial. En este sentido, se exige que el sistema de denuncias garantice que sólo el órgano destinatario acceda a su identidad; precisamente para preservarla pero, sobre todo, para evitar que se tomen represalias frente al informante.

En efecto, el hecho de que un trabajador informe de cualquier irregularidad conlleva el tratamiento de los datos personales, de modo que se debe garantizar, por una parte, que la información recogida y tratada se transmita exclusivamente a las personas responsables de la investigación, y por otra, que se adopten las medidas necesarias para realizar el seguimiento e investigación de los hechos denunciados[19].

Por tanto, los sujetos que reciban esta información (personas o departamento designado al efecto), deben asegurar que se maneja de forma confidencial y se adoptan las medidas de seguridad, preservando la identidad del denunciante y los derechos del denunciado en cuanto a información, acceso, rectificación, cancelación y oposición. El art. 24. 4 LOPD añade, a este respecto, que los datos personales deben conservarse en el sistema de denuncias por el tiempo imprescindible "para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados". En todo caso, transcurridos tres meses desde de la introducción de los datos, se debe proceder a supresión del sistema de denuncias[20].

Además del deber de confidencialidad, los denunciantes deben estar protegidos frente a todo tipo de represalias, ya sean directas o indirectas, que se tomen, alienten o toleren por el empresario, clientes o destinatarios de servicios y personas que trabajen por cuenta o en nombre de éstas, incluidos los compañeros de trabajo y directivos de las misma organización o de otras organizaciones en las que el denunciante esté en contacto en contexto de sus actividades.

El Capítulo VI de la Directiva 2019/1937 recoge las medidas de protección del informante en el ámbito laboral. Siguiendo la Recomendación del Consejo Europeo sobre

[19] S. RODRÍGUEZ ESCANCIANO: *Derechos laborales digitales: garantía e interrogantes*, Ed. Aranzadi, 2019, pag. 115.

[20] "Salvo que la finalidad de la conservación sea dejar evidencia funcionamiento del modelo de prevención de la comisión de delito por la persona jurídica" (art. 24. 4 LOPD).

whistelblowers[21], se proponen, entre otras, las siguientes medidas: prohibición de represalias (art. 19), medidas de apoyo (art. 20), medidas de protección frente a represalias (art. 21), medidas para la protección de las personas afectadas (art. 22) y sanciones.

En definitiva, se establece una suerte de indemnidad que trata de garantizar una protección cualificada al trabajador que denuncia una irregularidad en el seno de la empresa. En este sentido, el legislador europeo se esfuerza por identificar todas aquellas situaciones que pudieran suponer un trato desfavorable para el trabajador, cuando la decisión disciplinaria del empresario sea consecuencia de la denuncia del trabajador.

Se incluyen tanto la amenaza de represalia como la tentativa de represalia, en forma de: 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 con respecto a sus resultados laborales; f) imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias; g) coacciones, intimidaciones, acoso u ostracismo; h) discriminación, o trato desfavorable o injusto; i) no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo 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 sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector; m) terminación anticipada o anulación de contratos de bienes o servicios; n) anulación de una licencia o permiso; o) referencias médicas o psiquiátricas.

Desde la perspectiva europea se ofrece una protección amplia y adecuada, que debe vincularse a la exigencia general de que las represalias por el hecho de la denuncia se consideren una vulneración de un derecho fundamental o libertad pública[22]. En este sentido, consideramos que todos los actos "de represalia", consecuencia de la información de irregularidades transmitida por el denunciante, deberían reputarse nulos y sin efecto, tanto si consisten en decisiones unilaterales del empresario o como si proceden de un tercero del "contexto laboral". En esta línea el Tribunal Constitucional, en su STC 146/2019, de 25 de septiembre, declara vulnerado el derecho a la libertad de expresión del trabajador que es despedido disciplinariamente por criticar la gestión empresarial del centro de trabajo en el que prestaba servicios. Distingue entre el derecho a expresar y difundir libremente los pensamientos ideas y opiniones, del derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión [art. 20.1 a) y d) CE].

El Alto Tribunal nos recuerda su doctrina consolidada sobre el derecho que garantiza la libertad de expresión, cuyo objeto son los pensamientos, ideas y opiniones (concepto amplio que incluye las apreciaciones y los juicios de valor) y el derecho a comunicar información, que se refiere a la difusión de aquellos hechos que merecen ser considerados noticiables. Tal distinción entre pensamientos, ideas y opiniones, de un lado, y comunicación informativa de hechos, de otro, tiene una importancia decisiva para determinar la legitimidad del ejercicio de esas libertades, pues, «mientras los hechos son susceptibles de prueba, las opiniones o juicios de valor, por su misma naturaleza, no se prestan a una demostración de exacti-

[21] Protecting Whistleblowers, Council of Europe, Recommendation, CM/Rec(2014), en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806fffd1

[22] J.F. LOUSADA AROCHENA: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *cit.*, pág 9.

tud, y ello hace que al que ejercita la libertad de expresión no le sea exigible la prueba de la verdad o diligencia en su averiguación, que condiciona, en cambio, la legitimidad del derecho de información» (FJ 4º STC 146/2019).

Por todo ello, el TC centra su enjuiciamiento en el marco del derecho a la libertad de expresión y rechaza la interpretación del derecho fundamental realizada por TSJ del País Vasco que, "al haber exigido que la crítica realizada no trascendiera más allá de la empresa, despojó al trabajador de la libertad de expresión que le reconoce el art. 20.1 a) CE, haciendo que tal derecho cediera ante un deber de lealtad entendido en términos absolutos de «sujeción indiferenciada del trabajador al interés empresarial» (SSTC 4/1996, de 16 de enero, FJ 4, y 227/2006, de 17 de julio, FJ 5) (FJ 6º STC 146/2019).

Ahora bien, la prohibición de represalia frente al denunciante no debe impedir la adopción de las medidas disciplinarias cuando la investigación interna determine que la comunicación sea falsa y que la persona que la ha realizado ha actuado de mala fe[23].

Así, lo ha entendido el TSJ de Andalucía, en sus sentencia de 15 de marzo de 2018, al no reconocer la vulneración del derecho a la indemnidad por la sanción a un trabajador que no cumple con una orden reiterada de la empresa para justificar irregularidades anunciadas por él y presuntamente cometidas por otros miembros de la empresa con repercusiones sobre su bienestar emocional[24].

Como se ha señalado, la norma no exige que el denunciante actúe de buena fe, pero requiere que éste afirme o crea en la veracidad de las irregularidades denunciadas. El hecho de que el trabajador haya mantenido una aptitud obstativa para verificar las irregularidades por él informadas, quiebran la protección frente a represalias y le excluye, por tanto, de la aplicación de la garantía de indemnidad. En efecto, la divulgación de informaciones, aún siendo veraces, no puede realizarse con el ánimo exclusivo de "vilipendiar, humillar o insultar a las personas de forma innecesaria o gratuita, o *con el ánimo de* inferir intencionalmente un daño moral o material al empleador"[25].

Salvo error u omisión por nuestra parte no hemos encontrado jurisprudencia del Tribunal Supremo que haya examinado las represalias frente a las denuncia del trabajador *(whistleblowing)* como vulneración de un derecho fundamental[26]. Sin embargo, hemos revisado con resultados positivos la doctrina judicial de algunos Tribunal Superiores de Justicia que estiman la existencia de vulneración de los derechos fundamentales del trabajador por denuncia de irregularidades.

– Este es el caso de la STSJ de Madrid, de 15 de febrero de 2019, que reconoce la existencia de acoso moral *(whiselblowers)* a un

[23] S. Rodríguez Escanciano: *Derechos laborales digitales: garantía e interrogantes, cit.*, pag. 116.

[24] STSJ Andalucía 15 marzo 2018 (rec 1935/2017).

[25] J.F. Lousada Arochena: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *cit.*, pág 10.

[26] En todo caso, la doctrina laboralista advirtió en la STC 6/1998, de 21 de enero, una recepción de la figura del *whistleblower* y de la necesidad de protección que ésta requiere, en S. Del Rey Guanter: *Libertad de expresión e información y contrato de trabajo: un análisis jurisprudencial*, Ed. Civitas, Madrid, 1994, p. 100-102. En efecto, se apuntan muchos de los requisitos que ahora exige la Directiva comunitaria, a saber: a) relevancia pública de la información que, en el caso de las administraciones públicas, e extiende a cualquier tipo de irregularidad; b) diligencia en la verificación de los hechos denunciados, y en fin, c) no se exige que la divulgación de la información esté sujeta a un procedimiento formal, ni tampoco se exige que el denunciante acuda los órganos administrativos o judiciales competentes. En este caso, sí se observa un cambio, pues ahora es necesario que los denunciantes acudan a los sistemas de denuncia previstos (interno o externos) para que no se adopten represalias hacia al trabajador. Otro sector de la doctrina ahonda en esta línea, al entender que la STC 204/1997, de 25 de noviembre y la precedente STC 6/1998, de 21 de enero, "trasponen al derecho español una figura de procedencia norteamericana, *whistleblower* o denunciante, en J. Gorrelli Hernández, T. Igartúa Miro: "La liberta de información y contrato de trabajo. El problema de sus límites. A propósito de la STC 57/1999, de 12 de abril", *Revista Doctrinal Aranzad Social, Vol. BIB, 1999/343.*

tripulante de cabina de una compañía aérea por el colectivo de pilotos. Conviene recordar y repasar por su trascendencia y alcance para el tema que nos ocupa, los hechos que dan lugar a la vulneración de derechos fundamentales y al reconocimiento de una indemnización al trabajador en conceptos de daños y perjuicios.

El día 8 de enero de 2017 en el vuelo de la compañía aérea el actor presencia la comisión por el comandante de vuelo de dos irregularidades que afectan sustancial y gravemente a la seguridad del vuelo. En su condición de sobrecargo deja constancia al comandante de la irregularidad y de la más absoluta disconformidad de toda la tripulación ante las mismas. El otro comandante que irregularmente viaja en cabina de vuelo y que no forma parte de la tripulación de ese vuelo con dos de sus hijos y con otro menor en trasportín situado en galley trasero junto a puerta en asiento exclusivo de tripulación de forma agitada y agresiva le indica que debe acatar órdenes.

El actor denuncia la irregularidad el mismo día 8 de enero de 2017 marcando expresamente la casilla "request confidentiality", es decir, solicita confidencialidad. En el indicado modelo consta su nombre. El 23 de febrero de 2017 la empresa abre pliego de cargos al comandante del vuelo por las irregularidades cometidas en el vuelo del 8 de enero de 2017 como responsable de la seguridad de todos los miembros de la tripulación y le suspende por falta leve con 1 día de empleo y sueldo. A partir de aquí se desata una campaña de persecución contra el demandante por el colectivo de pilotos a través de whatsapps y otros medios llegando a decirle que no le iban a pasar ni una, que no querían que accediera a la cabina de tripulación, que no querían coincidir con él, que "Usted no puede pasarnos la comida, ni las bebidas, ni siquiera destapar la comida".

El 25 de julio de 2017 se informa al actor de la activación del procedimiento de actuación por acoso moral con las siguientes actuaciones: "1. investigación de los hechos denunciados que durará el tiempo estrictamente necesario para el esclarecimiento de los mismos. 2. Citarle para que comparezca en la fecha que se le dará a conocer próximamente, en el Servicio Médico de la Empresa, a fin de evaluar los daños que el supuesto acoso haya podido o pueda potencialmente ocasionarle". El actor no pasó el reconocimiento para evaluar su estado de salud al estar en incapacidad temporal.

El 28 de septiembre de 2017, una vez concluidas las investigaciones, se le comunica por la demandada que no se ha detectado indicio racional alguno de acoso laboral, lo que ponemos en su conocimiento a los efectos que resulten oportunos, dando por resuelto el protocolo de acoso laboral o "mobbing"" con esa fecha.

El informe pericial recoge la presencia en el actor de una sintomatología cronificada y recurrente que se concreta en una serie de síntomas que aparecen en las pruebas aplicadas con síntomas psicosomáticos en forma de palpitaciones, ardores de estómago y molestias gástricas y dolor precordial, trastorno por estrés postraumático.

El Tribunal Superior de Justicia de Madrid considera una forma específica de acoso moral "aquel que sufren las personas que denuncian las irregularidades y/o disfunciones de un superior, sistema u organización (conocido como *whistleblower*)" pues, en muchas ocasiones, van a ser represaliadas por el sistema o por el grupo al que el superior pertenece. El que "informa" porque considera un deber, o simplemente cumple con el deber establecido de alertar y denunciar las acciones de sus compañeros de trabajo y/o superiores que representan una grave irregularidad o peligro sustancial y específico para la seguridad o la salud, se convierten con frecuencia en víctimas de represalias. En estos casos, el acoso va destinado a silenciar al que no participa del mismo juego que los demás y a represaliar al que ha hablado. Lo que le ocurre a un whistleblower es de todo punto equiparable al acoso moral. De ahí la necesidad de su protección a través de una confidencialidad estricta.

Como señala el propio TSJ, no se tiene una protección general de whistleblower, pero conviene en "que una mínima e indispensable ética organizacional y de prevención del riesgo psicosocial debe llevar a la protección del denunciante por cuanto la denuncia supone un beneficio tanto para la organización como para la sociedad en su conjunto al poner de manifiesto y sacar a la luz problemas que deben ser resueltos y respecto de los cuales muy pocas personas están dispuestas a hacer algo, especialmente cuando la irregularidad es cometida por algunos de los miembros de un grupo con poder y mando (en este caso el colectivo de pilotos)"[27].

El actor cumplió su deber y obligación de informar, requiriendo expresamente de su empleador protección específica por confidencialidad *(request confidentiality)*, depositando de buena fe confianza plena en la empresa [art. 5 a) ET], es decir, en la confianza legítima de que se preservaría la confidencialidad que la empresa, con toda evidencia, no garantizó adecuadamente en ningún momento. Por todo ello, y a juicio del Tribunal Superior de Justicia de Madrid, es indiferente quién llevó a cabo la filtración porque es la empresa la responsable frente al trabajador denunciante de preservar su confidencialidad y de garantizar que como consecuencia de la denuncia no sufra perjuicio alguno [art. 4.2.d) y e) ET].

Al igual que es responsable la empresa de la custodia y protección de los datos personales sin perjuicio de la acción que, en su caso, corresponda contra el filtrador[28]. Por tanto, el actor se ha visto sometido a violencia psicológica en el trabajo y fuera de él como consecuencia también del trabajo al no haber preservado la empresa la confidencialidad, violencia que se ha ejercido de forma sistemática y recurrente durante un tiempo prolongado, con la finalidad de destruir sus redes de comunicación, destruir su reputación, perturbar el ejercicio de sus labores y lograr finalmente que termine abandonando el lugar de trabajo, lo que ya ha acontecido siquiera temporalmente al causar incapacidad temporal[29].

Por todo ello, el Tribunal Superior de Justicia de Madrid entiende que nos encontramos ante un supuesto de *whistelblowing*. El denunciante solicitó confidencialidad en la denuncia de irregularidades, aquélla no se garantizó en ningún caso; y además, supuso

[27] La pérdida del beneficio o contemplar al denunciante como un peligro es la causa de la represalia y el acoso. Al respecto sirva de ejemplo el documento interno de la OIT para su personal titulado "La ética en la oficina: la protección de los funcionarios que denuncian irregularidades" destinado a la protección de los funcionarios que consideran que fueron objeto de represalias por haber denunciado casos de falta grave o por haber colaborado en una auditoría o una investigación. En determinados sectores, como es el de la seguridad en la aviación civil, existen normas específicas que tratan de favorecer la denuncia y proteger al denunciante. Tal es el caso del Reglamento (UE) nº 376/2014 relativo a la notificación de sucesos en la aviación civil. De forma expresa los considerandos de la norma exponen que la persona física que notifique un suceso que afecte a la seguridad debe estar adecuadamente protegida, careciendo la notificación de sucesos de la identificación y los datos del notificante, sin que quede registro en las bases de datos (STSJ 15-02-2019, Rec. 824/2018).

[28] Entender lo contrario llevaría a considerar que si la empresa no conoce el origen de la filtración o de cualquier irregularidad que en su seno se cometa deviene irresponsable de todo punto lo que escapa a la más elemental lógica de la responsabilidad empresarial. No es de recibo, por tanto, la afirmación judicial de que el actor no prueba que la empresa tuviera conocimiento del autor de las filtraciones, porque lo decisivo es que no preservó adecuadamente la confidencialidad, es decir, no protegió adecuadamente al trabajador en el origen de un riesgo laboral (art. 15.c LPRL). Este riesgo viene representado por la denuncia actuación que, por sí sola, se erige como un evidente riesgo laboral para la seguridad y la salud del trabajador por cuanto, formulada la denuncia, existe la posibilidad de que el trabajador sufra un determinado daño derivado del trabajo de producción racionalmente probable en un futuro inmediato y susceptible de causar un daño grave para su salud (art. 4.2º, 4º y 5º LPRL), en STSJ 15-02-2019, Rec. 824/2018.

[29] La expresión de esta violencia psicológica ha tenido lugar a través de diversos comportamientos hostiles de distinta naturaleza tanto contra su reputación como contra su dignidad con el objeto de crear estigma. Descriptivo al respecto es la declaración escrita del comandante donde explica cómo se niega a compartir mesa con el actor de forma reiterada, que pueda manipular la comida, y la caracterización del demandante como un buscador de problemas e, incluso, manipulador de situaciones para buscar blindajes laborales. El TSJ da credibilidad por la metodología utilizada al informe pericial y cuantifica la indemnización en 60.000 euros utilizando como parámetro analógico la LISOS, en STSJ 15-02-2019, Rec. 824/2018.

la pérdida de su reputación y confianza en el desarrollo de su relación de trabajo. De ahí que el Tribunal calificara las represalias por el hecho de la denuncia como vulneración de un derecho fundamental.

– En sentido similar, se pronuncia también el Tribunal Superior de Justicia de Madrid, en su sentencia de 15 de marzo de 2019, aunque ahora en un supuesto circunscrito a un caso de acoso sexual, ambiental reiterado y generalizado en el trabajo por un superior jerárquico, que se canaliza a través de una primera denuncia genérica e indeterminada y formulada ante un canal externo, gestionado también de forma externa a la empresa.

El TSJ revoca la sentencia de instancia y declara la procedencia del despido estimando el recurso de la empresa[30]. A juicio de la Sala de suplicación, se trata de una falta continuada y oculta como consecuencia de la situación personal del demandante en la empresa de la que por consiguiente se prevale, que responde a una conducta prolongada en el tiempo manifestada a través de una pluralidad de hechos y comportamientos repetidos, dotados de una unidad que se corresponde con el mismo tipo de infracción.

En el presente supuesto, a criterio del Tribunal Superior de Justicia, nos encontramos ante la imputación de un acoso sexual ambiental llevado cabo por la persona que ostenta la máxima responsabilidad y representa, en consecuencia, los valores de la dirección y de la mercantil demandada. La propia naturaleza de la imputación impide el registro sistemático y minucioso de cada uno de los hechos que integran la conducta, a la sazón continuada. Así, entiende el Tribunal que resulta prácticamente impensable exigir a las trabajadoras que lleven a cabo un registro diario de cada uno de los comentarios inapropiados que reciben a los efectos de conformar, si es el caso, una denuncia de acoso sexual ambiental. Varios son los argumentos que se señalan en la sentencia y fundamentan tal situación de discriminación y las dificultades de su denuncia, entre otras:

– "Las relaciones humanas, entre ellas las laborales, se deben desarrollar y normalmente se desarrollan en los límites de la confianza, el respeto y la igualdad.

– La sutileza de muchos de los comportamientos de acoso y su ambigüedad buscada incluso de propósito, impide que el afectado procese inmediatamente y sin duda la violencia del comportamiento del que está siendo objeto, que normalmente se cuestiona por temor a la incomprensión.

– De la misma forma impide la reacción inmediata, probablemente en la esperanza de que son hechos aislados, por no hablar de la dificultad de reacción cuando el que la lleva a cabo representa la máxima autoridad empresarial lo que constituye una agravante.

– Por el contrario, es la repetición, la constancia, la actuación sobre multiplicidad de sujetos pasivos la que genera el daño, el efecto indeseado, humanamente y jurídicamente reprobable y que en un momento dado elimina la sutileza y la ambigüedad, esto es, la duda de la violencia que es objeto de denuncia.

Por ello, a juicio del TSJ de Madrid, resulta evidente la dificultad y casi imposibilidad del registro de hechos y fechas en supuestos como el presente pues, de exigirse, se impediría la

[30] A la vista de que la primera denuncia es genérica e indeterminada y formulada ante un canal externo gestionado también de forma externa a la empresa, no entra en juego el mecanismo de la prescripción del art. 60 del ET, que ha resultado así infringido por la sentencia de instancia Además, es necesario reiterar que, en modo alguno, las denuncias pueden ser medio de prueba de infracciones laborales que, desde luego, requerirán de una labor investigadora más seria por la propia entidad antes de proceder a las imposición con las garantías previstas en el art. 58 ET y en el convenio que resulte de aplicación, en S. RODRÍGUEZ ESCANCIANO: *Derechos laborales digitales: garantía e interrogantes*, *cit.*, pag. 116.

persecución de esos "pequeños" actos violentos cotidianos que pueden parecer incluso "normales" para algunas personas y en algunos contextos, que empiezan con sencillas faltas de respeto y que poco a poco aumentan en intensidad especialmente si el grupo social en el que aparecen no reacciona, pues es entonces cuando los actos progresivamente se conviertan en verdaderas conductas violentas susceptibles de generar graves consecuencias. En fin, en las circunstancias expuestas, exigir aquel registro minucioso penalizaría la reacción del grupo que ha sido, en definitiva, el motor de la denuncia del Presidente del Comité de Empresa.

El actor ha llevado a cabo acoso sexual físico al besar en el cuello[31]; también ha llevado a cabo acoso sexual de palabra al comentar sus fantasías sexuales[32] o realizar comentarios sobre lo bien que les sientan los pantalones o la ropa que visten las trabajadoras[33]. Estos actos son ejemplos de un comportamiento degradante continuo y son considerados como conducta violenta en el trabajo (Acuerdo Marco sobre violencia y acoso en el trabajo). Constituyen acoso sexual y, como tales, sin más precisiones, son reputados como falta muy grave habiendo decidido la empresa la sanción de despido en uso de un poder de elección no revisable judicialmente. Sin duda inciden en la dignidad y degradan a la mujer y el ambiente laboral. El hecho de que el ambiente de trabajo sea aún así normal[34] no constituye un obstáculo porque lo decisivo es que el factor que incide en el ambiente sea degradante, no que el ambiente esté ya degradado.

Y, efectivamente, es degradante al constituir las conductas descritas factores susceptibles de deteriorar o degradar el ambiente laboral al afectar negativamente las acciones de acoso sexual del máximo responsable empresarial en España de forma directa o indirecta, voluntaria o involuntariamente, a la calidad ambiental laboral de la empresa demandada en cualquiera de sus grados.

Como señala el Acuerdo Marco sobre el acoso y la violencia en el trabajo "el respeto mutuo de la dignidad a todos los niveles en el lugar de trabajo es una de las características esenciales de las organizaciones exitosas. Por eso son inaceptables el acoso y la violencia… en todas sus formas… que puede tener graves consecuencias sociales y económicas. Tanto el Derecho de la UE como el nacional establecen el deber de los patronos de proteger a los trabajadores contra el acoso y la violencia en el lugar de trabajo".

En fin, concluye el Tribunal Superior de Justicia de Madrid que "la política de tolerancia cero hacia este tipo de conductas, plasmada de la misma forma en el Convenio, determina la declaración de procedencia del despido y la consiguiente corrección del proceder empresarial en aplicación del art. 54.g) ET, 16.m del Acuerdo y 57.m del Convenio de aplicación."

-Además de la identificación de la existencia de vulneración de los derechos fundamentales del trabajador por denuncia de irregularidades, resulta interesante también que se contemple como represalia los daños reputacionales "en especial, en los medios sociales que pueda ser objeto el *whistleblowers*", así como las denominadas "listas negras" que impliquen el denunciante no pueda volver a trabajar en un determinado sector.

Tal es el caso de la STS, Sala Primera, de 12 de noviembre de 2015[35], en la que incorpora un criterio de interés, tras analizar los efectos de la inclusión de un trabajador en una "lista negra" que le vetaba para trabajar para empresas del sector de las telecomunicaciones.

En efecto, el demandante, trabajador de una empresa subcontratista de Telefónica, fue despedido acusado de haber cobrado a un cliente por un servicio que debía ser gratuito.

[31] Hechos probados octavo y décimo.
[32] Palabras textuales: "hacer un trío o tocar los pechos".
[33] Hechos probados octavo y décimo.
[34] Hechos probado noveno.
[35] Sentencia nº 609/2015.

Demandó a su empresa por dicho despido, que fue declarado improcedente por la jurisdicción social por no quedar acreditados los hechos imputados y la empresa optó por indemnizarle y extinguir la relación laboral. Posteriormente, el trabajador realizó varios procesos de selección y cuando iba a ser contratado por una empresa del mismo sector, ésta le manifestó que no podía contratarle, por haber sido incorporado a un fichero de "personal conflictivo" por los hechos que motivaron su despido –a pesar de que el Juzgado no los considerara probados[36].

Finalmente, el Tribunal Supremo ha considerado que efectivamente se había producido la vulneración de su derecho al honor y a la protección de datos (reconocidos en el art. 18 CE) –no así a su propia imagen–, y condena a la empresa a abonar la suma de 30.000 euros. El Tribunal estima la demanda basándose en que la prueba de que efectivamente existía tal "lista negra" resultaba prácticamente imposible para el trabajador. De hecho, además de los indicios derivados de los fallidos procesos de selección, la única prueba que pudo aportar en el juicio fue la testifical de un miembro del comité de empresa de Telefónica que mostró su convencimiento de que "existía ese fichero de trabajadores vetados".

Sin embargo, el Tribunal considera que, tratándose de un procedimiento de vulneración de derechos fundamentales, y habida cuenta de la existencia de tales "indicios razonables", la carga de la prueba debe recaer en la empresa que supuestamente incluyó sus datos en la "lista negra", que debería haber tratado de demostrar en el acto de juicio –cosa que no hizo– que cuando notificó a Telefónica la extinción de la relación laboral con el trabajador (comunicando para ello sus datos de carácter personal), no incluyó ningún otro tipo de información sobre los hechos que motivaron el despido.

Desde el punto de vista de la normativa de protección de datos, el Tribunal considera que la cesión de datos realizada para la formación de la "lista negra" fue ilícita, ya que a) no contó con el consentimiento del afectado; b) no resultaba amparada en ninguna de las excepciones del artículo 11.2 LOPD; c) no respetaba el principio de calidad de los datos –los datos cedidos no eran veraces, al no haber sido considerados por el Juzgado de lo Social como acreditados–; y d) no se lo concedió la posibilidad de ejercitar los derechos acceso, rectificación, cancelación y oposición. Además, para el Tribunal, esta infracción de la normativa de protección de datos produjo, a su vez, una vulneración del derecho al honor del demandante, ya que los datos comunicados no cumplían el requisito de veracidad y afectaban negativamente a su reputación.

Desde el punto de vista del Derecho del Trabajo, el Tribunal no cuestiona en esta sentencia la competencia de la jurisdicción civil para conocer de la acción interpuesta. Ahora bien, cabe entender que si la demanda se interpusiese a la luz de la LRJS, la competencia sería, a buen seguro, de la jurisdicción social.

La Sala Primera tampoco entra a valorar aquí ni si el consentimiento prestado por el ex trabajador hubiese sido válido en este contexto, ni tampoco qué hubiese sucedido en el supuesto de que los hechos imputados en la carta de despido hubieran resultado acreditados y el despido hubiese sido declarado procedente.

Por último, se contempla también la asistencia al *whistleblower* en los procesos frente a las represalias, incluida la asistencia jurídica gratuita si procede, la protección frente a acusaciones de revelación de información confidencial, así como la obligación de inversión de carga de la prueba. Asimismo, se incluyen medidas de apoyo financiero y psicológico al denunciante (art. 20 DPII)[37].

[36] Como consecuencia de ello, el trabajador demandó a su anterior empleador solicitando una indemnización de más de 600.000 euros por la vulneración de sus derechos de honor e imagen, así como a la protección de datos personales.

[37] Asimismo, y para lograr la protección efectiva del *whistleblower* y favorecer que se recurra a los canales de

4. A MODO DE CONCLUSIÓN

Es pronto para valorar la incidencia de la Directiva 2019/1937 en el marco de la protección de datos y el contexto laboral. Habrá que esperar a la norma de transposición que desarrolle los mínimos establecidos para garantizar una cultura de cumplimiento y lucha contra la represión de la información de las irregularidades.

En todo caso, la detallada regulación de los canales de denuncia y, a su vez, la minuciosa configuración de las medidas de protección para el *whistleblower* ofrece una respuesta razonable y proporcionada para aquéllos que deban hacer uso de estos sistemas de información para denunciar infracciones en el ámbito laboral.

El art. 17 ET recoge una garantía de indemnidad amplia, reputando nulas las órdenes del empresario que supongan un trato favorable de los trabajadores como reacción ante una reclamación efectuada en la empresa o ante una decisión administrativa o judicial destinada a exigir el cumplimiento del principio de igualdad de trato y no discriminación.

Sería deseable que la Ley de transposición de la Directiva acogiera un precepto legal que garantizara al trabajador el derecho a no sufrir perjuicio alguno por el hecho de formular denuncias o quejas de anomalías o irregularidades de la empresa. Esta obligación se podría exigir al empresario, siempre que la empresa hubiera habilitado un adecuado sistema de canal denuncia, en el que se asegure tanto la confidencialidad del denunciante como la garantía de no sufrir represalias por presenta una queja o denuncia.

denuncia de irregularidades, se contemplan sanciones frente a aquellas entidades que a) impidan o intenten impedir la presentación de denuncias, b) adopten medidas de represalia frente a los informantes, c) promuevan procedimientos temerarios contra los informantes, d) incumplan el deber de mantener la confidencialidad de la identidad de los informante (art. 23 DPII).

RESUMEN

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantías de los Derechos digitales se dicta para adaptar el ordenamiento jurídico español al Reglamento UE 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril, 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). Esta Ley introduce un sistema de información de denuncias que establece una especial protección para los denunciantes que va a desplegar efectos en el ámbito laboral. Estos sistemas de recepción y conocimiento de infracciones se encuadran bajo las exigencias de la legislación aplicable en materia de protección de datos, siempre que se traten denuncias referidas a normas, fundamentos principios, cuyo incumplimiento tenga consecuencias efectivas sobre la pervivencia de la relación contractual entre la empresa y el denunciado.

El art. 24 LOPD regula un sistema de denuncias internas desde la perspectiva del derecho de protección de datos personales, referido a los límites de acceso a los datos de las personas, la confidencialidad del tratamiento o la limitación temporal en orden a la conservación de las denuncias.

La Directiva UE2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, relativa a la protección de las personas que informan sobre infracciones del Derecho de la Unión configura, de una forma mucho más profusa, un sistema de canales de denuncia, externas e internas, que protege la confidencialidad, anonimato y no represalia del denunciante.

Estamos, pues ante una norma esperada, un elemento más en el engranaje normativo que el legislador comunitario –pero también, el nacional– propone para articular la obligación de establecer canales de denuncia y a la vez prevé medidas de protección que deben garantizarse en el marco del *whistelblowing*.

Su principal virtualidad es que, con su sola existencia, despeja los debates sobre los cauces del sistema de denuncia, aportando luz en un contexto absolutamente necesitado de seguridad jurídica. Se busca reforzar la protección del *whistelblower* y el ejercicio del derecho a la libertad de expresión e información, reconocidos en el art. 10 Carta Europea de Derechos Humanos y en el art. 11 de la Carta de Derechos Fundamentales.

Se delimitan las reglas de configuración del ámbito de aplicación, es decir, se delimitan las infracciones, así como también el ámbito personal de los denunciantes. Se protege no sólo a los denunciantes del sector privado, sino también del sector público, que comuniquen o revelen públicamente información sobre infracciones del Derecho de la Unión, que se hayan conocido en un contexto laboral, siempre que tuvieran motivos razonables para creer que la información era veraz en el momento de la denuncia.

Las denuncias deben articularse a través de unos sistemas establecidos al efecto. Se prevén tres tipos de canales: internos, dentro de una entidad jurídica pública o privada; 2) externos, dependientes de las autoridades que se designen en cada Estados miembros, y con los que la empresa tendrá cierta prevención, sobre todo, por temor "a perder la reputación" y 3) la revelación pública, que consiste en la puesta a disposición del público de información sobre infracciones.

Con este sistema de denuncias habrán de tenerse muy presente las medidas de protección del denunciante. La primera es la confidencialidad, es decir, los canales de denuncia deben estar diseñados y gestionados de tal forma que este deber debe alcanzar también a los no afectados, para que su acceso a la información sea del todo imposible al tratarse de personal "no autorizado", pero también se deben establecer garantías frente a posibles represalias en el ámbito laboral. No obstante, antes de que se apliquen las

medidas protectoras frente a posibles desagravios del trabajador por haber informado de determinadas irregularidades en la empresa, debe comprobarse que el denunciante cree en la veracidad de los hechos que denuncia y que procede a través de los cauces adecuados. Los informantes deben estar protegidos frente a todo tipo de represalias, ya sean directas o indirectas, que se tomen por el empresario, clientes incluso compañeros de trabajo. Se propone: la prohibición de represalias, medidas de apoyo, medidas de protección frente a represalias, medidas para la protección de las personas afectadas y sanciones. En definitiva, se establece una suerte de indemnidad que trata de garantizar una protección cualificada al trabajador que denuncia una irregularidad en el seno de la empresa.

Ahora bien la prohibición de represalia frente al denunciante no debe impedir la adopción de las medidas disciplinarias cuando la investigación determine que la comunicación sea falsa y que la persona que la ha realizado ha actuado de mala fe.

En todo caso, la prohibición frente a represalias debe tramitarse como vulneración de un derecho fundamental del trabajador y tales medidas deberían reputarse nulas y sin efecto. Aunque todavía no se ha pronunciado el Tribunal Supremo sobre el particular, sí que hemos revisado con resultados positivos la doctrina judicial de algunos Tribunales Superiores de Justicia que estiman la existencia de vulneración de derechos fundamentales del trabajador por denuncia de irregularidades. En este sentido, la doctrina del Tribunal Constitucional ha confirmado la recepción de la figura del *whistelblower* y la necesidad de protección que ésta requiere.

Todavía es pronto para valorar la incidencia de la Directiva 2019/1937 en el marco de la protección de datos y el contexto laboral. Habrá que esperar a la norma de transposición que desarrolle los mínimos establecidos para garantizar una cultura de cumplimiento y lucha contra la represión de la información de las irregularidades. En todo caso, es una estupenda oportunidad para que el legislador español promueva una regulación detallada y completa sobre *whistleblowing* a tenor de la doctrina que sobre este particular está construyendo el Tribunal Constitucional.

Palabras clave: Tecnologías; informantes; Canal de denuncias; confidencialidad; derecho fundamental; prohibición de represalias

ABSTRACT The Law 3/2018 of 5th December about the protection of personal data and guarantees of digital rights is approved to adapt the Spanish legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) This Law introduces a reporting information channel or system that establishes special protection for whistleblowers that will display effects in the workplace

This Law introduces confidential and secure reporting channels and by ensuring that whistleblowers are protected effectively against retaliation, even in the work-related context. Specifically, art. 24 Law about the protection of personal data and guarentees of digital rights regulates an internal reporting channel from the perspective of data protection, referring to the limits of access to people's data, the confidentiality of the treatment or the temporary limitation in order to preserve internal reporting

Recently, it has adopted 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 sets up a system of reporting channels, external and internal, that protects the confidentiality, anonymity and non-retaliation of the reporting person.

This Directive is an expected norm, one more element in the normative gear that the community legislator – but also our national one – proposes to articulate the obligation to establish reporting channels and provides protection measures that must be guaranteed within the framework of the *whistelblowing*. Its main virtuality is that it clears the debates on the reporting channels finding out ways of solution in a context which requires legal certainty. It´s try to strengthen the protection of the whistelblower and the exercise of the right to freedom of expression and information, recognized in art. 10 European Charter of Human Rights and in art. 11 of the Charter of Fundamental Rights

The rules of configuration of the scope of application are defined, as well as the personal scope of the reporting persons. It wil be apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context about violations of Union Law, including reasonable suspiciones, whic ocured or are very likely to occur ein the organisation in which reportung person Works or has worked or in another organisation with which the reporting person i sor was in contact through his or her work, and about attempts to conceal such breaches.

Information on breaches must be articulated through reporting channels established for this purpose. Three types of channels are planned: internal reporting channel, within a public or private legal entity; 2) external reporting channel, dependent on the authorities competent are designated in each Member States, and with whom the company will have some prevention, especially for fear "to lose reputation" and 3) public disclosure, which consists in putting public provision of information on breaches.

With this reporting system the reporting person should enjoy the protection against retaliation provided by this Directive. The first is confidentiality, that is, the reporting channels must be designed and managed in such a way that this duty must also reach those not authorised staff members competent to receive or follow up on reports, because they are "unauthorized" personnel; but it should be established guarantees possible retaliation in the work-related context that, in any case, must be processed as a violation of a fundamental right of the worker, in fact such measures should be considered void and without effect.

However, before the protective measures are applied to prohibit any form of realiation against reporting persons for having reported certain irregularities in the company, it must be verified that the informan believes in the veracity of the facts he denounces and that he proceeds through the appropriate channels Informants must be protected against all types of realiation, whether direct or indirect, that are taken by the employer,

clients or third persons who are connected with the reporting persons. The proposal are: prohibition of retaliation, measures of support, measures for protection against retaliation, measures for the protection of concerned persons and penalties sanctions. In short, a kind of indemnity is established that tries to guarantee a qualified protection to the worker who informas on breaches within a privat or public company.

The prohibition of retaliation against reporting persons should not prevent the adoption of disciplinary measures when the investigation determines that the communication is false and that the person who has informed about it has acted in bad faith.

The prohibition of retaliation must be processed as a violation of a fundamental right and such measures should be considered void

Although the Supreme Court has not yet ruled on the matter, we have reviewed with positive results the judicial doctrine of some Superior Courts of Justice, that consider the existence of a violation of fundamental rights of the worker for reporting information on breaches. In this sense, the doctrine of the Constitutional Court has confirmed the reception of the figure of the *whistelblower* and the need for protection that it requires.

It is early to analyse the impact of Directive 2019/1937 in the framework of data protection and on the work-related context. We will have to wait for the transposition regulation that develops the minimum established to guarantee the protection of persons who report breaches of Union law. In any case, it´s a great opportunity for the Spanish legislator to adopt a complete and detailed regulation on whistleblowing, according to the doctrine that the Constitutional Court is building on this particular.

Keywords: Technologies; information on breaches; reporting channels-confidentiality; fundamental right; prohibition of retaliation