TRATADOS

La concreción nacional del Reglamento General de Protección de Datos mediante la Ley Orgánica de Protección de Datos y de garantía de los derechos digitales, de 5 de diciembre de 2018 ha generado, en los últimos tiempos, especificaciones nacionales relevantes sobre múltiples aspectos que requieren un mayor estudio por parte de la doctrina.

En la presente obra colectiva se acomete un estudio acerca de aquellas cláusulas abiertas más destacadas que ha adoptado el legislador español en nuestro ordenamiento jurídico, así como los efectos de su implementación en otras normativas sectoriales en España. Esta se estructura en tres secciones: la primera incluye aspectos transversales y de primer orden relativos a salud y diversidad, especialmente, aquellos relacionados con la pandemia que provocó la irrupción de la Covid-19. La segunda examina la relación entre el derecho a la transparencia y a la protección de datos de carácter personal. Por último, en el tercer bloque se contemplan algunas de las cláusulas abiertas directamente relacionadas con cuestiones internacionales actuales que inciden en el derecho a la protección de datos.

tirant
lo blanch

tirant
lo blanch

CRISTINA PAUNER CHULVI, ROSARIO GARCÍA MAHAMUT
BEATRIZ SUSANA TOMÁS MALLÉN
Editoras

+Lectura GRATIS en la nube

LA IMPLEMENTACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN ESPAÑA Y EL IMPACTO DE SUS CLÁUSULAS ABIERTAS

LA IMPLEMENTACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN ESPAÑA Y EL IMPACTO DE SUS CLÁUSULAS ABIERTAS

CRISTINA PAUNER CHULVI
ROSARIO GARCÍA MAHAMUT
BEATRIZ SUSANA TOMÁS MALLÉN
Editoras

JORGE AGUSTÍN VIGURI CORDERO
Coordinador

tirant
lo blanch

TRATADOS

PROTECCIÓN DE LAS PERSONAS INFORMANTES EN LA DIRECTIVA (UE) 2019/1937 Y TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. BREVE REFERENCIA A LA LEY 2/2023 DE PROTECCIÓN DE LAS PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN

Cristina PAUNER CHULVI[1]
Catedrática de Derecho Constitucional
Universitat Jaume I

I. INTRODUCCIÓN

El 7 de octubre de 2019, el Consejo de la Unión Europea aprobó la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión[2] (en adelante, la Directiva). Con esta norma, la Unión Europea se une a las políticas de protección de los informantes que se están impulsando en los últimos años en el entorno internacional y nacional para hacer frente a un tipo de criminalidad que se desarrolla en el seno de las organizaciones y entidades públicas o privadas.

Se parte de la idea de que la detección y prevención de las actividades ilícitas que puedan darse en estas corporaciones es mucho más eficaz si se cuenta con la colaboración de personas que, por formar parte de la organización, están en una posición privilegiada para conocer aquellas irregularidades pero que el miedo a las represalias que pudieran padecer las silencia. Para evitar estas situaciones, se incorporan nuevas herramientas que protegen a los potenciales denunciantes, informantes o alertadores[3].

La Directiva promueve este tipo de políticas y establece la obligatoriedad de crear canales de denuncia de cualquier posible incumplimiento o irregularidad relacionada con el Derecho de la Unión en el ámbito público y privado y establece unas normas mínimas de

1 El presente trabajo ha sido realizado en el marco de los proyectos de investigación RTI2018-095367-B-I00 del Ministerio de Ciencia e Innovación y PID2021-128309NB-I00 del Ministerio de Ciencia, Innovación y Universidades.

2 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 (DO L 305 de 26.11.2019) https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32019L1937

3 Con estas tres expresiones se alude a las personas que denuncian o revelan información sobre ilícitos o actividades irregulares en organizaciones y entidades públicas o privadas. A lo largo del texto se utilizará el término "informante" por ser el que ha empleado definitivamente la Ley que regula la incorporación al Derecho español de la Directiva y a la que nos referimos más adelante.

protección para la persona informante frente a las posibles represalias que se produzcan dentro de su entorno laboral[4]. Para procurar favorecer el flujo de información se asegura precisamente la protección del informante con la confidencialidad además de otras medidas que intentan garantizar su inmunidad.

En alusión al objetivo principal que persigue, la Directiva es también conocida como Directiva de protección de denunciantes o, más popularmente, Directiva *whistleblowing* o *whistleblowers.* Esta última expresión literalmente traducida significa "los que soplan el silbato": se trata de quienes alertan de que se han producido ciertas irregularidades en el seno de la organización y su finalidad es que, tras la alerta interna, sea la propia empresa la que investigue y actúe en consecuencia. Debe, por tanto, desecharse cualquier interpretación negativa de este término que pudiera relacionarlo con la delación o la actuación policial y relacionarlo con la seguridad pública y la prevención e investigación de la actividad ilícita[5].

Aunque se han construido numerosas definiciones del informante, el documento elaborado por la Comisión Europea, denominado *Frequently Asked Questions: Whistleblower protection* ("FAQ") (2018)[6] y que acompañaba 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".

---

[4] No obstante, la Directiva no es un sistema de protección general al informante de cualquier actividad ilícita sino que es un sistema de protección en un ámbito especial ya que recae sobre unas concretas materias que se detallan expresamente en su artículo 2 (la contratación pública, los servicios, productos y mercados financieros, el blanqueo de capitales, la financiación del terrorismo, la seguridad de los productos, la seguridad de transporte, la protección del medioambiente, la protección frente a las radiaciones y seguridad nuclear, la seguridad de los alimentos, la sanidad y bienestar de los animales, la salud pública, la protección de los consumidores, la protección de la privacidad y datos personales, la seguridad de las redes y los sistemas de información, los intereses financieros de la Unión Europea, así como las infracciones relativas al mercado interior).

[5] Porque, ciertamente, el término *whistleblower* podría traducirse en español como "chivato" o "soplón" aunque estos términos tienen un matiz peyorativo que no se comparte en el significado de este vocablo en inglés. Sobre la figura del *whistleblower* en la experiencia de *common law* puede verse Francesca Masiero, A., "La disciplina del whistleblowing a la luce della direttiva 2019/1937/UE. Tra prevenzione dei fenómeno corruttivi e tutela del denunciante", *Archivio Penale*, n. 2, 2020, pp. 1-30 concretamente pp. 2 a 5, y bibliografía allí citada. Al origen de la palabra, ligado a la imagen virtuosa que lo acompañaba, y su posterior evolución, se refiere Benítez Palma, E., "El control externo y el *whistleblowing* (canales de denuncia)", *Revista Española de Control Externo*, vol. XX, n. 59, 2018, pp. 13 a 16. En general, remitimos a las reflexiones realizadas en torno al concepto por Pérez Triviño, J. L., "Whistleblowing", *Eunomia. Revista en Cultura de la Legalidad*, n. 14, 2018. Disponible en https://e-revistas.uc3m.es/index.php/EUNOM/article/view/4170/2694.

[6] Disponible en https://ec.europa.eu/commission/presscorner/detail/es/MEMO_18_3442. En términos similares, el documento-resumen que acompañaba a la Propuesta de Directiva, denominado *Fact sheet on whistleblower protection* ("Fact sheet") (2018), 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 Estados Unidos y otros países anglosajones se ha desarrollado una larga cultura de *whistleblowers*, especialmente intensa en la década de 1960[7], mediante la implantación de sistemas y programas de buen gobierno (programas de *compliance*) cuya finalidad es prevenir o, al menos, reducir la comisión de actos ilícitos en su funcionamiento. Posteriormente, la lucha contra corrupción comenzó a incluirse en la agenda de los grandes organismos internacionales desde los años 90 y fue poco a poco incorporándose en iniciativas nacionales, entre ellas España, hasta llegar a la actualidad que ya es una de las grandes preocupaciones a nivel social, económico y político[8]. La Directiva responde, precisamente, a este impulso e intenta luchar eficazmente contra este tipo de comportamientos delictivos poniendo en el centro de la regulación la protección de informantes cuya colaboración para sacar a la luz conductas corruptas o ilícitas es esencial. La Directiva se conceptúa como una norma armonizadora de mínimos por lo que deja margen a las legislaciones nacionales para fijar reglas más favorables o protectoras del informante.

El plazo de transposición de la Directiva venció el pasado 17 de diciembre de 2021 para las empresas de más de 250 trabajadores y existe un segundo plazo –hasta el 17 de diciembre de 2023– para las empresas de entre 50 y 249 trabajadores.

En España, el termino finalizó sin que contásemos con la norma de transposición[9], pero finalmente se ha aprobado la Ley 2/2023, de 20 de febrero, reguladora de la protección de

---

7 Ragués i Vallés, R., "¿Héroes o traidores? La protección de los informantes internos (wistleblowers) como estrategia político-criminal", *InDret*, n. 3, 2006, pp. 3 y ss. Las primeras normas que fijaron un estatuto de protección de los informantes surgieron en Estados Unidos, destacamente, la *Loyd-La Follette Act* de 1912, la *Whistleblower Protection Act* de 1989, la *Sarbanes-Oxley Act* de 2002 y la Dodd-Frank Act de 2010 siendo esta última una de las más favorables para la protección de los d informantes sobre tres elementos básicos: protección laboral, anonimato y recompensas al delator (Blanes Soliva, M. F. y Meco Tébar, F., "La protección de datos de las personas denunciantes en casos de corrupción en el sistema español", *Cuadernos de Política Criminal*, n. 129, 2019, p. 155).

8 Pueden verse los Informes de Evaluación sobre España del grupo de Estados contra la Corrupción del Consejo de Europa (GRECO) que siguen reportando incumplimientos de nuestro país (https://www.coe.int/en/web/greco/evaluations) o el grado de preocupación social por la corrupción que, con fluctuaciones, se mantiene entre los principales problemas para la ciudadanía en las encuestas y barómetros del CIS (https://www.cis.es/cis/opencm/ES/11_barometros/index.jsp). A nivel global pueden consultarse los índices de percepción de la corrupción en todos los países en los Informes que elabora Transparencia Internacional (https://transparencia.org.es/indice-de-percepcion-de-la-corrupcion/).

9 Es oportuno advertir sobre los riesgos que el retraso en el deber de transposición de estas disposiciones a la legislación nacional ya que crea situaciones de inseguridad jurídica y puede suponer la apertura de procedimientos sancionadores por la UE. España es uno de los países europeos con más procedimientos de infracción abiertos según el Informe de la Comisión de Control de la aplicación del derecho de la Unión Europea (*Informe anual 2019*, Bruselas, 31.7.2020, COM (2020)350 final, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0350&from=ES) y ha sido condenada por el retraso en la transposición de la Directiva 2016/680 de protección de datos en investigaciones penales. En la STJUE asunto C-658/19, de 25 de febrero de 2021, el Tribunal expresa de manera taxativa la falta de diligencia del caso español y la especial gravedad del retraso por tratarse de normas que garantizan el buen funcionamiento del espacio de libertad, seguridad y justicia dentro de la Unión. Sobre esta cuestión, véase Navarro Mejía, I., "La falta de transposición de una directiva europea en materia reservada a ley orgánica. Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea de 25 de febrero de 2021. Asunto C-658/19", *Revista de las Cortes Generales,* n. 111, 2021, pp. 611-628.

las personas que informen sobre infracciones normativas y de lucha contra la corrupción[10] (en adelante la Ley 2/2023).

En cualquier caso, como reconoce Viguri Cordero, "cada Estado miembro ha contado con tiempos distintos que han girado en torno a consultas y reflexiones de calado sobre cómo las legislaciones nacionales deben encajar el marco jurídico europeo existente. A modo de ejemplo, países como Francia o Irlanda se han enfrentado a procesos de revisión de sus legislaciones ya consolidadas con el objetivo de que estas guarden coherencia con la citada Directiva e incrementen la efectividad de las disposiciones de protección al informante. Sin embargo, países como España comenzaron prácticamente desde cero, un punto de arranque en fase inicial que ha requerido de mayores esfuerzos en la adopción de una ley nacional de protección al *whistleblower*".[11]

La Ley 2/2023 se refiere igualmente al trascendente papel de las personas informantes y su Exposición de Motivos apela a la colaboración ciudadana como elemento indispensable para la eficacia del Derecho y la vincula, entre otros, al principio constitucional de sometimiento de todos los poderes públicos y de la ciudadanía al ordenamiento jurídico (artículo 9.1 CE). En particular, relaciona esa colaboración ciudadana con la obligación general de la ciudadanía de denunciar la comisión de delitos de los que se tenga conocimiento y el reconocimiento de acciones públicas de impulso de la investigación en diversas áreas (medio ambiente, urbanismo, patrimonio histórico-artístico) [12].

Asimismo, destaca que ha habido numerosos ejemplos de actuaciones cívicas que, poniendo sobre aviso de la comisión de actos irregulares y de corrupción, permitieron impulsar investigaciones e imponer sanciones penales tras el correspondiente procedimiento judicial. Pero también son conocidas las penosas consecuencias que se derivaron de aquellas acciones de clara utilidad pública para quienes denunciaron[13].

Quizá la novedad más destacable de la Ley 2/2023 es que su ámbito de aplicación es más extenso que el de la Directiva, configurada como norma de mínimos tal y como señalamos arriba. Así, además de proteger a quienes informen sobre las infracciones de Derecho de la Unión que marca la Directiva, amplía el amparo y abre los canales de

---

10 BOE núm. 44, de 21 de marzo de 2023.

11 Viguri Cordero, J., "El marco jurídico europeo de protección del whistleblower: un derecho nacional emergente", en *Aspectos problemáticos en las relaciones entre el Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea y derecho interno*, C. Sánchez Hernández, M. Fernanda Palma, O. García Pérez, I. Ferreira Leite (dirs.), Tirant lo Blanch, Valencia, 2023 (pendiente de publicación).

12 Impulso que también se ha producido en el Derecho de la UE donde determinados sectores cuentan con normas específicas sobre la denuncia de infracciones. Así, en la regulación europea de servicios financieros, la prevención del blanqueo de capitales y la financiación del terrorismo, la seguridad del transporte o la protección del medio ambiente. En relación con estas normas europeas, la Directiva se aplicará subsidiariamente (Rodríguez-Medel Nieto, C., "La protección de los informantes – whistleblowers – y las garantías de los investigados. Análisis de la propuesta de Directiva de la Unión Europea y en España de la proposición de ley integral de lucha contra la corrupción y protección de los denunciantes", *Revista de Estudios Europeos*, n. extraordinario monográfico 1/2019, p. 228).

13 En este sentido, se puede consultar el listado elaborado por la Fundación Hay Derecho que incluye numerosos casos de informantes de corrupción en España que han sufrido represalias por sus denuncias. Fundación Hay Derecho, *Derechos de denunciantes: análisis de casos*, https://www.hayderecho.com/protegiendo-a-los-valientes/derechos-de-denunciantes-analisis-de-casos/

comunicación a quienes adviertan de vulneraciones del ordenamiento nacional, pero limitado a las penales y a las administrativas graves o muy graves para concentrar la actividad de los canales internos y externos en las vulneraciones que se consideran que afectan con mayor impacto al conjunto de la sociedad[14].

El establecimiento de los canales de comunicación o denuncia internos es una pieza clave en la implantación de un modelo efectivo de cumplimiento normativo (o de *compliance*)[15] con el que evitar la comisión de delitos o responsabilidades posteriores[16]. Este modelo experimentó un gran impulso tras la reforma del Código Penal en 2015, que introdujo una cláusula de exención de responsabilidad penal para aquellas personas jurídicas que hubiesen adoptado un modelo eficaz de prevención de riesgos penales (o de *compliance*) Entre otros requisitos, para que un modelo de prevención de delitos sea considerado eficaz de acuerdo con el artículo 31 bis. 5 del CP, debe imponer a los integrantes de la persona jurídica la obligación de informar de posibles incumplimientos a través de un canal de denuncias. La Directiva traslada ese sistema de cumplimiento normativo también al sector público mediante la exigencia de creación de los canales de denuncia, considerados además como uno de los pilares que conforman los sistemas de integridad, un elemento esencial para el bienestar económico y social y para la prevención de la corrupción[17].

Resulta evidente que la corrupción es una amenaza a la democracia, desprestigia a los poderes públicos y a las instituciones en que se encarnan, socava la confianza de los ciudadanos y, en última instancia, puede suponer la deslegitimación del Estado[18]. El coste

---

14 Esta previsión deja fuera del régimen de especial protección de los informantes aquellas infracciones del ordenamiento jurídico frente a incumplimientos de normas de Derecho privado que regulan relaciones entre particulares y que, por tanto, no afectan al adecuado funcionamiento de las instituciones públicas y privadas.

15 El sistema de *compliance* o cumplimiento normativo "es un mecanismo preventivo que sirve para liberar de responsabilidad a las personas jurídicas". Comprende los modelos de organización o gestión que las personas jurídicas deben implementar para autorregularse y fijar los límites a partir de los cuales se puede considerar una actuación de esa empresa como delictiva. La importancia de tener un sistema de compliance radica en que si la empresa consigue probar en la investigación penal a la que es sometida que ha cumplido con las normas de su propia autorregulación, quedará libre de toda culpa y por tanto exenta de responsabilidad criminal (Vázquez de Castro, E., "La doble faceta de la protección de datos personales en los sistemas de compliance", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 59, 2022).

16 La responsabilidad penal de las personas jurídicas está recogida por el Código Penal español desde 2010. Desde ese año, las organizaciones responden por los delitos que hayan cometido sus trabajadores y directivos, siempre y cuando tengan como resultado un cierto beneficio para la entidad. Sobre la responsabilidad penal de las personas jurídicas y los programas de *compliance*, por todos, véase Gómez Colomer, J. L. (dir.) y Madrid Boquín, C. M. (coord.), *Tratado sobre Compliance Penal. Responsabilidad penal de las personas jurídicas y modelos de organización y gestión*, Tirant lo Blanch, Valencia, 2019.

17 Sobre el tema, véase Villoria Mendieta, M., "Un análisis de la Directiva (UE) desde la ética pública y los retos de la implementación, *Revista Española de la Transparencia*, n. 12, 2021, pp. 15-24; Jiménez Sánchez, F., "Los efectos de la corrupción sobre la desafección y el cambio político en España", *Revista Internacional de Transparencia e Integridad*, n. 5, 2017, pp. 1-16 y Jiménez Asensio, R., *Marcos de integridad y códigos de conducta: encuadre conceptual y algunas buenas prácticas*, y bibliografía allí citada. Disponible en https://laadministracionaldia.inap.es/noticia.asp?id=1506999

18 Sobre la corrupción como amenaza a la democracia existen numerosos estudios entre los que destacamos, Nieto, A., *Corrupción en la España democrática*, Ariel, Madrid, 1997; Vidal-Beneyto, J., *La corrupción de la democracia*, Catarata, Madrid, 2010; Bustos Gisbert, R., "Corrupción política: un análisis

social de la corrupción es muy elevado porque tiene un impacto negativo sobre la política y la convivencia de un país. Pero también tiene un coste económico que es difícil de calcular porque incluye no solo la cuantía de los fondos públicos desviados sino también deteriora elementos clave del funcionamiento de la economía como la pérdida de la producción debida a la mala asignación de recursos; el falseamiento de los incentivos; el desinterés por el emprendimiento, la innovación, la competencia y el esfuerzo y otras ineficacias[19]. Por eso, la lucha contra la corrupción a través de la denuncia y una adecuada protección del informante se vincula directamente con la promoción de la transparencia, rendición de cuentas y buen gobierno a los que complementa[20].

El principio democrático de transparencia –en su vertiente activa y pasiva– actúa como un buen antídoto contra los actos de corrupción. Así, la publicidad activa a la que se somete a la Administración y entes del sector público les obliga a poner a disposición del público y mantener actualizada la información que generan en ejercicio de su competencia. Por su parte, el acceso a la información pública permite que cualquier persona solicite la información pública que no forma parte de las obligaciones de transparencia y aquella debe ser proporcionada salvo causas tasadas cuando perjudique a ciertos intereses o afecte a determinada información. No es descartable que, por no publicarse o no solicitarse, la información sobre actuaciones irregulares o ilegales no lleguen a conocimiento de quien tenga capacidad para adoptar medidas contra tales prácticas[21]. Estas, sin embargo, pueden ser detectadas por personas que, de tener interés en su erradicación, cuentan con la denuncia como herramienta eficaz para comunicar violaciones y abusos de derecho que dañen el interés público y que de otra forma hubieran permanecido ocultos.

A su vez, la transparencia conecta directamente con la rendición de cuentas puesto que es esta la finalidad a la que sirve: "apoderar a la ciudadanía para que pueda ejercer ese control democrático de naturaleza horizontal (o "vertical ascendente") sobre el poder político; mejor dicho, de la actuación de las administraciones públicas"[22].

---

desde la teoría y la realidad constitucional", *Teoría y Realidad Constitucional*, monográfico n. 25, 2010, pp. 69-109; Villoria Mendieta, M., Gimeno Feliu, J. M.; Tejedor Bielsa, J. (dirs.), *La corrupción en España. Ámbitos, causas y remedios jurídicos*, Atelier, Barcelona, 2016; Betacor, A. (dir.), *Corrupción, corrosión del Estado de Derecho*, Aranzadi y Thomson Reuters, 2017.

19 López Donaire, B., "Marcos de integridad y los canales de denuncia. El derecho a la buena administración", en *La Directiva de protección de los denunciantes y su aplicación práctica al sector público*, J. Gimeno Bevià y B. López Donaire (eds.), Tirant lo Blanch, Valencia, 2022, p. 102.

20 En este sentido, Clemente Martínez, destaca como el hecho de que un cargo público alerte sobre casos de corrupción supone un acto de valentía y permite, en la práctica, el cumplimiento de principio de buen gobierno de informar sobre las posibles irregularidades detectadas, que se encuentra recogido en la normativa sobre buen gobierno (Clemente Martínez, J., "Los principios de buen gobierno de la nueva ley valenciana 1/2022", *Estudios De Deusto*, vol. 70, n. 2, 2022, pp. 135-136). CORREGIR TAMAÑO DE LA NOTA

21 Aliaga Rodríguez, R., "La denuncia anónima como instrumento de transparencia y protección de los denunciantes", *Revista Española de la Transparencia*, n. 14, 2022, p. 60.

22 Jiménez Asensio, R., "Instituciones de garantía de la transparencia", *El Cronista del Estado social y democrático de Derecho*, n. 68, 2017, p. 65. Con más detalle, el mismo autor explora la construcción de marcos de integridad institucional y el fortalecimiento la transparencia como vías en la lucha contra la corrupción en Jiménez Asensio, R., *¿Cómo prevenir la corrupción? Integridad y transparencia*, Catarata, Madrid, 2017.

Por su parte, el buen gobierno como tercer eje de toda acción política se basa en una gestión de calidad de lo público y una reacción contra el paradigma de la mala administración, esto es, la corrupción[23]. El control de la Administración no debe basarse únicamente en el control ex post y en cómo limitar su poder, sino que debe ampliarse a la gestión de los recursos y a los mecanismos de control preventivos para frenar las malas prácticas y en definitiva la corrupción. Las denuncias permiten colaborar a la ciudadanía en ese control y deben ser consideradas una herramienta para hacer efectivos los principios jurídicos de buen gobierno y un instrumento de realización efectiva del derecho a una buena administración.

Las líneas que siguen a esta Introducción se estructuran en cuatro apartados. En primer lugar, comenzamos por un estudio de la protección de la persona informante desde la perspectiva constitucional donde se indicará cómo incide ese estatuto protector en los derechos fundamentales de la ciudadanía. A continuación, se analizan las diferencias que existen entre la denuncia anónima y la denuncia confidencial puesto que se ha producido una evolución respecto a su admisión, aunque en ambos casos debe quedar completamente asegurada la inmunidad del informante. El siguiente apartado examina las medidas contenidas en la Directiva y la Ley 2/2023 para garantizar la protección de los datos personales obtenidos a través de los canales de denuncias. Finalmente, se presenta una serie de reflexiones a modo de conclusión.

II. LA PERSONA INFORMANTE COMO OBJETO DE PROTECCIÓN DE LA DIRECTIVA DESDE LA PERSPECTIVA CONSTITUCIONAL

La protección que la Directiva proporciona a la figura del informante sirve para garantizar una serie de derechos fundamentales a los que la propia Directiva alude en sus Considerandos y que, desde la perspectiva constitucional, han sido avalados por la jurisprudencia europea y nacional.

Literalmente, la Directiva se refiere la garantía de numerosos derechos entre los que destacamos, en primer lugar, el derecho fundamental a la libertad de expresión o, con mayor precisión, el derecho a la información; en segundo término, el derecho a la privacidad y la protección de los datos de carácter personal y, en tercer lugar, el derecho a la tutela judicial efectiva. Aparte, es indudable la incidencia de esta regulación en otros derechos como el derecho a unas condiciones de trabajo justas y equitativas en cuanto que trata de proteger al informante frente a las represalias en el contexto laboral, la libertad de empresa o el derecho a una buena administración ya que la protección contra todo perjuicio que pueda derivarse a los ciudadanos por una revelación pública también conecta con el principio democrático de transparencia y la rendición de cuentas. A la mayoría de

[23] Sobre el tema, por todos, véase Tomás Mallén, B., *El derecho fundamental a una buena administración,* INAP, Madrid, 2004.

ellos –y algunos más– se refiere la Directiva que, a modo de recapitulación, los enumera en el Considerando 102[24].

Comenzando por las libertades informativas, el Considerando 31 de la Directiva afirma que "Las personas que comunican información sobre amenazas o perjuicios para el interés público obtenida en el marco de sus actividades laborales hacen uso de su derecho a la libertad de expresión" consagrado en el artículo 11 de la de la Carta de Derechos Fundamentales de la Unión Europea y el artículo 10 del del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Así, la protección que otorga la Directiva frente a represalias es un medio concreto de salvaguardar esa libertad de expresión.

Precisamente, las primeras sentencias dictadas en España en protección del trabajador-*informante* se pronunciaron a finales de los 80[25] y en ellas el Tribunal Constitucional resolvió recursos de amparo a favor de trabajadores que fueron objeto de despidos disciplinarios tras haber denunciado ilícitos cometidos en su empresa. El Alto Tribunal consideró que se había vulnerado el derecho a la libertad de información de los informantes[26]. Este derecho se consagra en el artículo 20 CE que distingue entre la libertad de expresión genérica (apartado 1.a) y el derecho a la información veraz y de interés público (apartado 1.d), separación que no se produce en la Carta que expone en el mismo apartado 1 de su artículo 11 que "Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras".

Como bien ha indicado la doctrina[27], el derecho implicado en los despidos de los informantes es el derecho a la información[28] siempre que revista las condiciones que

---

[24] Considerando 102: "La presente Directiva respeta los derechos fundamentales y los principios reconocidos, en particular, por la Carta, especialmente su artículo 11. En consecuencia, es esencial que la presente Directiva se aplique de conformidad con esos derechos y principios, garantizando el pleno respeto, entre otros, de *la libertad de expresión y de información, el derecho a la protección de los datos de carácter personal, la libertad de empresa, el derecho a un elevado nivel de protección de los consumidores, el derecho a un alto nivel de protección de la salud humana, el derecho a un alto nivel de protección medioambiental, el derecho a una buena administración, el derecho a la tutela judicial efectiva y los derechos de defensa".* La cursiva es nuestra.

[25] A pesar de la inexistencia de leyes específicas de protección a los informantes, el Derecho laboral español era la vía para la salvaguarda de los trabajadores ya que no admite como razón de despido procedente el hecho de que un trabajador haya cumplido con sus deberes ciudadanos de impedir futuros delitos o denunciar los ya consumados (Ragués i Vallés, R., "¿Héroes o traidores? La protección de los informantes internos (wistleblowers) como estrategia político-criminal", *cit.,* p. 10). Sobre la cuestión, por todos, véase Del Rey Guanter, S., *Libertad de expresión e información y contrato de trabajo: un análisis jurisprudencial*, Civitas, Sevilla, 1994.

[26] Seguimos a Martínez Saldaña, D.; Abril Martínez, J.; Rodríguez Celada, E. y Reyes Rico, L. I., "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. 29 y ss.

[27] Guamán Hernández, A., *La libertad de información del trabajador*, Tirant lo Blanch, Valencia, 2005, citada en Martínez Saldaña, D.; Abril Martínez, J.; Rodríguez Celada, E. y Reyes Rico, L. I., "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", *cit.,* p. 30.

determina el artículo 20.1.d) CE para gozar de protección constitucional, a saber, la veracidad y el interés público. Así, el derecho a la libertad de información de los trabajadores ampara "la difusión de hechos, datos o informaciones relativas a la empresa, máxime cuando sean de interés general, cuando puedan afectar a los consumidores o usuarios o cuando saquen a la luz pública irregularidades o actos ilícitos", siempre que la información transmitida sea "veraz", se respete la buena fe contractual y no se vulnere la prohibición de revelar datos secretos, reservados o confidenciales"[29].

La paradigmática STC 6/1988, de 21 de enero, concede el amparo por violación del derecho fundamental a la información de un periodista de la Oficina de Prensa del Ministerio de Justicia que había sido despedido a causa de unas declaraciones hechas a una agencia de noticias en las que reconocía la existencia de filtraciones de la Oficina a una concreta editora de prensa. El TC amparó su derecho de informar que había ejercido correctamente puesto que se trataba de (1) información veraz, (2) rectamente obtenida y difundida, y (3) de relevancia pública, elementos que la Directiva también recoge como condición para otorgar la protección al informante quien (1) ha de tener "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" (artículo 6.1.a), (2) debe difundirlos por los medios adecuados [canal interno, canal externo o revelación pública a medios (artículo 6.1.b)], y (3) ha de informar sobre cuestiones que tengan relevancia pública que, a los efectos de la Directiva, son las que afectan a intereses de la Unión (artículo 2).

La Directiva también se refiere a la defensa del pluralismo de los medios a través de la protección jurídica del informante cualquiera que sea la vía por la que este actúe[30]. Efectivamente, la norma europea establece una prelación[31] en la que, en primer lugar,

---

28 Aunque en ocasiones también se declare nulo un despido a consecuencia de la vulneración de la libertad de expresión. En este sentido puede verse la STC 146/2019, de 25 de noviembre, que declara nulo por vulneración del derecho a la libertad de expresión el despido de un trabajador que planteó una serie de quejas contra su empresa ante un ayuntamiento, incluso después de plantearlas previamente ante dicha empresa. El TC considera que el trabajador en ningún momento transgredió con sus manifestaciones los límites del derecho a la libertad de expresión puesto que, referidas estrictamente a cuestiones relativas al desarrollo de su relación laboral en el centro de trabajo, con ellas no se constató la utilización de expresiones ultrajantes u ofensivas que pudieran resultar impertinentes e innecesarias para el fin pretendido. Otros pronunciamientos sobre despidos que se producen tras el ejercicio de la libertad de expresión o de información del trabajador en STC 56/2008, de 14 de abril; STC 151/2004, de 20 de septiembre; STC 126/2003, de 30 de junio; STC 57/1999, de 12 de abril; y STC 126/1990, de 5 de julio.

29 Martín Valverde, A., Rodríguez-Sañudo Gutiérrez, F. y García Murcía, J., *Derecho del trabajo*, Tecnos, Madrid, 2005, 14.ª ed., p. 622.

30 Considerando 45: "La protección frente a represalias como medio de salvaguardar la libertad de expresión y la libertad y el pluralismo de los medios de comunicación debe otorgarse tanto a las personas que comunican información sobre actos u omisiones en una organización («denuncia interna») o a una autoridad externa («denuncia externa») como a las personas que ponen dicha información a disposición del público, por ejemplo, directamente a través de plataformas web o de redes sociales, o a medios de comunicación, cargos electos, organizaciones de la sociedad civil, sindicatos u organizaciones profesionales y empresariales".

31 Considerando 33: "En general, los denunciantes se sienten más cómodos denunciando por canales internos, a menos que tengan motivos para denunciar por canales externos. Estudios empíricos demuestran que la mayoría de los denunciantes tienden a denunciar por canales internos, dentro de la

obliga a contar con canales internos de comunicación a entidades jurídicas del sector privado y del sector público porque se considera que es preferible que la información sobre prácticas irregulares se conozca por la propia organización para corregirlas o reparar lo antes posible los daños.

La Directiva también reconoce que uno de los principales factores que desalienta a los potenciales informantes es la falta de confianza en la eficacia de las comunicaciones. Por ello, además de tales canales internos, en segundo lugar, exige la determinación de otros canales de comunicación externos, con el fin de ofrecer a los ciudadanos una comunicación con una autoridad pública especializada cuya actuación esté presidida por los principios de independencia y autonomía en la recepción y tratamiento de la información sobre las infracciones, lo que les puede generar más confianza al disipar su temor a sufrir alguna represalia en su entorno. La Directiva deja margen a las legislaciones nacionales sobre la configuración de estas autoridades a las que se refiere como "autoridades competentes"[32]. En el caso de España, la Ley 2/2023 contempla la creación de un nuevo organismo de naturaleza administrativa denominado Autoridad Independiente de Protección del Informante, A.A.I., adscrita al Ministerio de Justicia, entre cuyas funciones se incluye la potestad sancionadora de las infracciones cometidas en el ámbito del sector público estatal y del sector privado cuando la infracción o el incumplimiento informado afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma (artículos 42 a 59 de la Ley 2/2023).

Finalmente, y en determinados casos[33], el informante puede optar por la revelación pública (Considerandos 78 a 81) y poner esa información a disposición del público bien

---

organización en la que trabajan. La denuncia interna es también el mejor modo de recabar información de las personas que pueden contribuir a resolver con prontitud y efectividad los riesgos para el interés público. Al mismo tiempo, el denunciante debe poder elegir el canal de denuncia más adecuado en función de las circunstancias particulares del caso. Además, es necesario proteger la revelación pública de información, teniendo en cuenta principios democráticos tales como la transparencia y la rendición de cuentas, y derechos fundamentales como la libertad de expresión y la libertad y el pluralismo de los medios de comunicación, al tiempo que se encuentra un equilibrio entre el interés de los empresarios en la gestión de sus organizaciones y la defensa de sus intereses, por un lado, y el interés de los ciudadanos en que se los proteja contra todo perjuicio, por otro, conforme a los criterios desarrollados por la jurisprudencia del TEDH".

[32] El Considerando 64 sugiere, no obstante, que "dichas autoridades competentes podrían ser autoridades judiciales, organismos de regulación o de supervisión competentes en los ámbitos específicos de que se trate, o autoridades con una competencia más general a escala central dentro de un Estado miembro, autoridades encargadas del cumplimiento del Derecho, organismos de lucha contra la corrupción o defensores del pueblo". Un interesante análisis sobre los modelos de autoridades externas para la gestión de los canales externos de denuncias en Sierra Rodríguez, J., "Impulso europeo al whistleblowing y las autoridades de integridad", *Eunomía. Revista en Cultura de la Legalidad*, n. 19, 2020, pp. 64-85.

[33] Para que puedan acogerse a las medidas de protección de la Directiva, las personas que pongan la información a disposición del público deben cumplir alguna de las condiciones siguientes: a) que hayan denunciado primero por los canales internos y externos, sin que se hayan tomado medidas apropiadas en los plazos fijados por la Directiva; b) que tengan motivos razonables para pensar que la infracción puede constituir un peligro inminente y manifiesto para el interés público o, en el caso de denuncia externa, cuando exista un riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso. La Ley 2/2023 descarta estos requisitos para ofrecer protección a la persona que haga una revelación pública (artículo 28).

directamente a través de plataformas web o redes sociales, o acudiendo a representantes electos, organizaciones civiles, sindicales, profesionales o empresariales o a los medios de comunicación. El periodismo de investigación se beneficia y nutre de la información que los informantes les suministran, lo que redunda en un beneficio colectivo ya que permite a la prensa desarrollar la función de perro guardián de las instituciones democráticas[34]. A su vez, las personas que revelen infracciones quedan amparadas directamente por el secreto profesional de los periodistas tal y como estipula el artículo 15.2 de la Directiva[35] en relación con lo que dispone el Considerando 27 que permite, entre otros, a los profesionales de la comunicación acogerse a protección al amparo de la Directiva "cuando comunican información protegida por las normas profesionales aplicables, siempre que la comunicación de dicha información sea necesaria a los efectos de revelar una infracción que entre dentro del ámbito de aplicación de la presente Directiva".

En relación con el respeto a la privacidad y la protección de los datos de carácter personal, el Considerando 14[36] recuerda que están amparados como derechos fundamentales en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea y que las revelaciones de los informantes pueden servir para su protección cuando, por ejemplo, revelen infracciones sobre incidentes que afecten a la seguridad de las redes y los sistemas de información ya que "Dichas denuncias contribuyen a garantizar la continuidad de servicios esenciales para el funcionamiento del mercado interior y el bienestar de la sociedad".

No es necesario subrayar la importancia de que el tratamiento de los datos de carácter personal en la gestión del canal de denuncias se realice con total observancia de las reglas

---

[34] Considerando 46: "En especial, los denunciantes constituyen fuentes importantes para los periodistas de investigación. Ofrecer una protección efectiva a los denunciantes frente a represalias aumenta la seguridad jurídica de los denunciantes potenciales y de esta forma incentiva que se informe sobre infracciones también a través de los medios de comunicación. A este respecto, la protección de los denunciantes como fuente de informaciones periodísticas es crucial para salvaguardar la función de guardián que el periodismo de investigación desempeña en las sociedades democráticas".

[35] Artículo 15.2: "El presente artículo no se aplicará en los casos en que una persona revele información directamente a la prensa con arreglo a disposiciones nacionales específicas por las que se establezca un sistema de protección relativo a la libertad de expresión y de información".

[36] Considerando 14: "El respeto de la privacidad y la protección de los datos de carácter personal, amparados como derechos fundamentales en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), son otros ámbitos en los que los denunciantes pueden contribuir a la revelación de infracciones que puedan perjudicar el interés público. Los denunciantes también pueden ayudar a revelar infracciones de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo (19) sobre la seguridad de las redes y los sistemas de información que introduce el requisito de notificar incidentes, incluidos los que no pongan en peligro los datos personales, y requisitos de seguridad para las entidades que prestan servicios esenciales en numerosos sectores, por ejemplo la energía, la salud, el transporte y la banca, para los proveedores de servicios digitales clave, por ejemplo, servicios de computación en nube, y para los suministradores de bienes básicos como el agua, la electricidad o el gas. Las denuncias de los denunciantes en este ámbito son especialmente útiles a fin de prevenir incidentes de seguridad que afecten a actividades económicas y sociales fundamentales y a servicios digitales de uso generalizado, así como para prevenir toda infracción de las normas de la Unión en materia de protección de datos. Dichas denuncias contribuyen a garantizar la continuidad de servicios esenciales para el funcionamiento del mercado interior y el bienestar de la sociedad".

que determina el Reglamento Europeo de Protección de Datos (en adelante RGPD)[37]. Pautas que se orientan, básicamente, a garantizar la confidencialidad y que se concretan en los conocidos principios de licitud, lealtad, transparencia, minimización de datos, privacidad por defecto, etc. A esta cuestión dedicamos el apartado 4 al que remitimos.

Es interesante destacar que la relación entre el derecho a la protección de datos y los sistemas de cumplimiento normativo (*compliance*), de donde surgen los canales de denuncias y al que nos referimos arriba, es bifronte.

Por un lado, insistimos, la configuración del propio sistema de *compliance* ha de garantizar que el derecho a la protección de los datos de todas las personas implicadas – informante, denunciado y terceras partes – estará asegurada, vertiente que es la que nos interesa en este análisis.

Pero, por otro lado, el sistema de *compliance* en su función preventiva trata de evitar los incumplimientos normativos que generen cualquier tipo de responsabilidades a las organizaciones. Una de las más graves responsabilidades en las que puede incurrir una organización es la vulneración de derechos fundamentales, entre ellos, el de protección de datos. Esto quiere decir que las empresas han de garantizar la seguridad de los datos de carácter personal que manejen y responden, como personas jurídicas, incluso ante cualquier inactividad u omisión del deber de velar por la observancia de los derechos de protección de datos personales cuyo tratamiento se realice como consecuencia de su actividad. En los códigos de buenas prácticas y protocolos de las organizaciones han de diseñarse las medidas necesarias para que, en el tratamiento de datos personales de sus cargos directivos, trabajadores, usuarios, proveedores y terceros que se relacionen con ellas se respete su derecho a la protección de datos personales.

Por tanto y sintetizando, el derecho a la protección de datos personales es materia del propio proceso de *compliance* y también este derecho tiene que estar asegurado en los canales de denuncias.

Finalmente, y de manera destacada, la Directiva garantiza el pleno respeto al derecho a la tutela judicial efectiva y los derechos de defensa de todas las personas implicadas en la comunicación de un ilícito o irregularidad: tanto el informante como el denunciado y terceras partes afectadas.

Así, la Directiva despliega una serie de medidas de apoyo y protección a favor del informante, entre las que destacan: información y asesoramiento gratuitos respecto de los procedimientos y recursos disponibles y derechos y garantías de protección frente a represalias, asistencia efectiva por parte de las autoridades competentes, asistencia

[37] 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) (DO L 119 de 4.5.2016, p. 1), http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

jurídica en procesos judiciales, asistencia financiera y medidas de apoyo, incluido el apoyo psicológico[38].

Por otro lado, la Directiva impone medidas de protección de las personas denunciadas y exige que los Estados miembros velen por que los interesados disfruten plenamente de su derecho a la tutela judicial efectiva y a un juez imparcial, a la presunción de inocencia y al derecho de defensa, incluido el derecho a ser oídos, así como a acceder a su expediente, de conformidad con la Carta de Derechos Fundamentales de la UE (artículo 22.1), protegiendo en su caso también la propia identidad del interesado (artículo 22.2). Además, las mejoras nacionales que puedan introducir los Estados miembros a partir del contenido de mínimos de la Directiva tienen como límite la prohibición de interferir en las medidas para la protección de los investigados.

III. EL DEBATE EN TORNO A LA CONFIDENCIALIDAD Y EL ANONIMATO

La Directiva establece los requisitos para la gestión del canal de denuncias – interno o externo– y declara que deben ser "efectivos, confidenciales y seguros y garantizando la protección efectiva de los informantes frente a represalias" (Considerando 3). Específicamente, la configuración de estos sistemas de información debe satisfacer como exigencias mínimas un uso asequible, las garantías de confidencialidad[39] y las prácticas correctas de seguimiento, investigación y protección del informante. Asimismo, resulta indispensable para la eficacia de los sistemas internos de información la designación de un responsable de su correcto funcionamiento[40].

---

38 Estas medidas genéricas se concretan en la garantía de una indemnización o reparación real y efectiva, medidas provisionales adoptadas para poner fin a amenazas o represalias a la espera de resolución del proceso judicial iniciado tras la denuncia, la reversión de la carga de la prueba, la ayuda económica para sufragar los costes de los procesos judiciales penales a los que pudieran enfrentarse los informantes para defenderse de medidas de represalia contra ellos a través de procesos judiciales, entre otras.

39 El mantenimiento de la reserva de identidad obliga a un proceso de "seudonimización" de los datos personales que gestiona el canal de denuncias para proteger la confidencialidad del informante. La diferencia entre el proceso de seudonimización y el de anonimización es que la disociación de la identidad del afectado es reversible mientras que en el segundo no lo es y, por dejar de contener datos personales, la información ya no queda sometida a la normativa de protección de datos. Sobre el tema, véase Martínez García, D., "Anonimato, seudonimato y confidencialidad: Hacia un marco integral y coherente de protección de los alertadores", *Anuario del buen gobierno y de la calidad de la regulación: ABGCR*, n. 1, 2020 [Ejemplar dedicado a: La regulación de la protección de los alertadores y denunciantes (whistleblowers)], pp. 181-213.

40 La persona encargada de gestionar el canal de denuncias denominada responsable o delegado de compliance – *compliance officer* – puede ser personal propio de la empresa o un servicio externo contratado (véanse los argumentos a favor y en contra de cada opción en Curero, A., "¿Debe ser interna o externa la figura del 'compliance officer'?", *Actualidad Jurídica Aranzadi,* n. 938/2018, parte C, Cizur Menor, 2018). En las empresas pequeñas que se opte por un responsable de cumplimiento interno se permite que ejerza, además, las funciones de delegado de protección de datos. La equivalencia entre las funciones de ambos puestos es clara y la doctrina ha destacado el paralelismo que existe entre las medidas de garantía del derecho fundamental a la protección de datos personales que establece el RGPD y los mecanismos de compliance porque ambos responden a una visión preventiva frente a posibles incumplimientos y se subraya la necesidad de que los códigos de conducta o protocolos sobre protección

Los artículos 9 a 14 de la Directiva detallan esos principios inspiradores de las características que todo canal de denuncia debe tener. En concreto,

a) **Seguridad y confidencialidad:** su diseño, establecimiento y gestión deben ser seguros, impedir el acceso a la denuncia de personal no autorizado y garantizar la confidencialidad tanto del informante como de cualquier tercero mencionado en la denuncia (artículo 9.1.a y artículo 13.d).

b) **Celeridad**: se debe acusar recibo de la denuncia en el plazo de siete días y dar respuesta en un plazo no superior a 3 meses desde el acuse (artículo 9.1.b y f y artículo 11.2. b y d).

c) **Diligencia**: 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 y artículo 11.2.c).

Con esta última referencia, la Directiva no exige que se tramiten las denuncias anónimas[41] sino que, como norma de mínimos, deja que sean las leyes nacionales las que determinen si se aceptan o no y en qué condiciones (artículo 6.2)[42]. No obstante, la Directiva sí reconoce que las personas que hayan denunciado o revelado públicamente información sobre infracciones de forma anónima en un primer momento pero que hayan sido identificadas y sufran represalias posteriormente tienen derecho a la protección que se concede a los informantes en los mismos términos y con las mismas condiciones de los que se hayan identificado[43].

En España, la Ley 2/2023 admite que la comunicación de denuncias pueda llevarse a cabo con reserva de la identidad del informante o de forma anónima (artículo 17), criterio que cancela la posición mantenida por la Agencia Española de Protección de Datos que era contraria al anonimato por entender que la protección de la identidad de la persona informante estaba asegurada suficientemente mediante la confidencialidad. También el

---

de datos deben estar integrados en los códigos de buenas prácticas de la empresa para favorecer el control del tratamiento de los datos personales que maneja la organización y, en su caso, sea posible notificar cualquier incumplimiento a través del canal de denuncias (Vázquez de Castro, E., "La doble facetade la protección de datos personales en los sistemas de compliance", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 59, 2022).

41 Un completo alegato a favor de la denuncia anónima en Aliaga Rodríguez, R., "La denuncia anónima como instrumento de transparencia y protección de los denunciantes", *cit.,* pp. 57-78. Y en general, sobre la admisibilidad de la denuncia anónima, su evolución legal y jurisprudencial, puede verse Ortíz Pradillo, J. C., *Los delatores en el proceso penal. Recompensas, anonimato, protección y otras medidas para incentivar una "colaboración eficaz" con la justicia*, Wolters Kluwer, Madrid, 2018, pp. 73-84.

42 Considerando 34 de la Directiva (UE) 2019/1937: "Sin perjuicio de las obligaciones vigentes de disponer la denuncia anónima en virtud del Derecho de la Unión, debe ser posible para los Estados miembros decidir si se requiere a las entidades jurídicas de los sectores privado y público y a las autoridades competentes que acepten y sigan denuncias anónimas de infracciones que entren en el ámbito de aplicación de la presente Directiva. No obstante, las personas que denuncien de forma anónima o hagan revelaciones públicas de forma anónima dentro del ámbito de aplicación de la presente Directiva y cumplan sus condiciones deben gozar de protección en virtud de la presente Directiva si posteriormente son identificadas y sufren represalias".

43 Fundación Hay Derecho, *Estudio sobre los riesgos y recomendaciones para la transposición de la Directiva UE 2019/1937 en Cataluña sobre protección de los denunciantes de corrupción*, 2020, p. 30.

Grupo de Trabajo del Artículo 29 (en adelante GT29) defendía la denuncia no anónima[44], aunque la aceptaba con carácter excepcional. Así pues, la posibilidad de aceptar denuncias anónimas ha quedado totalmente consolidada, aunque la discusión en torno a su aceptación ha sido muy profusa.

El GT29 publicó el Dictamen 1/2006 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[45] en el que advertía que las empresas no deben fomentar la presentación de denuncias anónimas como manera habitual de presentar una queja y, más concretamente, no anunciarlo. La posibilidad de que se investiguen las denuncias anónimas queda como excepción[46]. Los argumentos que enumera el Dictamen para promocionar las informaciones suministradas bajo la identidad del informante o las denuncias confidenciales frente a las anónimas son los siguientes:

a) El anonimato no impide que otros adivinen con éxito quién planteó la cuestión;

b) Es más difícil investigar la cuestión si no se pueden realizar preguntas de seguimiento;

c) Es más fácil organizar la protección del informante frente a represalias, especialmente si dicha protección está dispuesta en la ley, si las cuestiones se plantean de manera abierta;

d) Los informes anónimos pueden llevar a las personas a centrarse en el informante, tal vez sospechando que plantea la cuestión con malicia;

e) La organización corre el riesgo de desarrollar una cultura de recibir informes anónimos de mala fe;

---

[44] Como explica Rallo Lombarte, ambos documentos surgen por los interrogantes que planteaba la aplicación de la Ley Sarbanes-Oxley a las filiales europeas que tenían muchas compañías estadounidenses de forma que quedaban obligadas a la creación de sistemas internos de denuncias – a riesgo de sufrir sanciones legales y multas en caso de incumplimiento – y el respeto a las previsiones sobre protección de datos personales contenidas en la entonces vigente Directiva 94/46 (Rallo Lombarte, A., "Whistleblowing (sistemas internos de denuncias) y protección de datos", en *Cuadernos de Derecho para Ingenieros. Cumplimiento normativo. Compliance*, La Ley-Wolters Kluwer, 2012, pp. 99 y 100).

[45] El GT29 es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018, fecha de entrada en vigor del RGPD que crea el Comité Europeo de Protección de Datos. 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/files/2006/wp117_en.pdf

[46] Al aceptar excepcionalmente la denuncia anónima, el GT29 enumera las condiciones bajo las que hacerlo: se debe informar al informante en su primer contacto que su identidad se mantendrá confidencial en todo el proceso y que no se divulgará a terceros, ni al denunciado ni a los mandos directivos del empleado – garantía de que su identidad se tratará de forma confidencial; si el informante persiste en la denuncia anónima, se aceptará; se anunciará a los informantes que puede ser necesario divulgar la identidad a las personas implicadas en cualquier investigación o procedimiento judicial posterior iniciado a resultas de la investigación; el tratamiento de denuncias anónimas será objeto de especial cuidado.

f) El clima societario dentro de la organización podría deteriorarse si los empleados son conscientes de que informes anónimos relativos a ellos podrían cursarse a través del programa en cualquier momento.

En la misma línea, el informe 128/2007[47] de la Agencia Española de Protección de Datos prohibió el envío de denuncias anónimas contrariamente a la regulación en otros países europeos. La Agencia, en referencia a los principios de exactitud y conservación recogidos en la entonces vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, defiende que debe evitarse la existencia de denuncias anónimas ya que es el tratamiento confidencial de las denuncias el que garantiza la exactitud e integridad de la información contenida en los sistemas de *whistleblowing*. A continuación, explica que la garantía de la confidencialidad protege suficientemente la identidad de la persona informante cuyos datos no podrán ser transmitidos en modo alguno al denunciado con ocasión del ejercicio del derecho de acceso. "Por ello – concluye — a fin de garantizar el cumplimiento del mencionado principio deberá exigirse que el sistema únicamente acepte la inclusión de denuncias en que aparezca identificado el informante, sin perjuicio de las salvaguardias que se han señalado para garantizar la confidencialidad de sus datos de carácter personal, no bastando el establecimiento de un primer filtro de confidencialidad y una posible alegación última del anonimato para el funcionamiento del sistema".

En cualquier caso, este debate quedó superado en España desde la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), precepto que será objeto de un análisis pormenorizado en el siguiente apartado.

El artículo 24.1 de la LOPDGDD señala que "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".

Como se ha advertido[48], el precepto anterior permite que se presenten denuncias de forma anónima en los canales internos de las entidades de Derecho privado. Sin embargo, la Directiva regula los canales de denuncia internos de las entidades del sector privado y del sector público, así como las denuncias externas. Y la Ley 2/2023 ha optado por admitir también la formulación de denuncias anónimas ante las "autoridades competentes" lo que incluye a la Fiscalía, el juez de Instrucción, la Policía, así que es fundamental preservar los derechos de tutela judicial y defensa también de las personas denunciadas.

Por este motivo, el artículo 16.2 de la Directiva, en relación con el Considerando 82, establece una excepción a la regla de la confidencialidad y solo permite divulgarse la

---

47 Agencia Española de Protección de Datos, *Informe 128/2007, de 1 de junio de 2007, de creación de sistemas de denuncias internas en las empresas (mecanismos "whistleblowers").* Disponible en https://www.aepd.es/es/documento/2007-0128.pdf

48 Martínez Saldaña, D.; Abril Martínez, J.; Rodríguez Celada, E. y Reyes Rico, L. I., "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", *cit.,* pp. 52 y 53.

identidad del informante u otra información en caso de que exista una obligación legal necesaria y proporcionada en el contexto de investigaciones llevadas a cabo por autoridades o de procesos judiciales, "en particular para salvaguardar el derecho de defensa de las personas afectadas"[49]. El artículo 33.3 de la Ley 2/2023, por su parte, también contempla esta excepción.

La jurisprudencia asimismo ha dejado atrás esta discusión manifestándose absolutamente a favor de las denuncias anónimas a las que considera una vía idónea para la revelación de la comisión de un hecho presuntamente delictivo y admite que sirvan de base para el inicio de una investigación penal (sentencias del Tribunal Supremo de 11 de abril de 2013, 6 de noviembre de 2017, 6 de febrero de 2019 y la renombrada sentencia de 6 de febrero de 2020, entre otras). Y existen múltiples entidades públicas que aceptan la denuncia anónima: desde universidades públicas (Universitat Jaume I, Universitat Pompeu Fabra) a organismos independientes (Oficina Antifraude de Cataluña, Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, Comisión Nacional del Mercados de Valores) pasando por corporaciones públicas (Ayuntamiento de Barcelona) y tantas otras.

Finalmente, y sin perjuicio de la plena admisibilidad de la denuncia anónima, se interpreta[50] que la denuncia no anónima aporta ciertas ventajas como la efectiva protección de los informantes contra posibles represalias en el ámbito laboral así como desde la perspectiva del derecho a la protección de datos[51]; la posibilidad de verificar la

---

[49] El Tribunal Supremo, con base en jurisprudencia del TEDH, ha restringido a casos excepcionales el mantenimiento del anonimato de los testigos en la fase de juicio oral para no comprometer el derecho de defensa del investigado. Concretamente, la sentencia de 4 de junio de 2019, declara: "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 [...]". Citado en Martínez Saldaña, D.; Abril Martínez, J.; Rodríguez Celada, E. y Reyes Rico, L. I., "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", *cit.*, p. 53.

[50] Entre otros, García Moreno, B., *Del whistleblower al alertador. La regulación europea de los canales de denuncia*, Tirant Lo Blanch, Valencia, 2020, pp. 285 a 287; Miranzo Díaz, J., "La nueva Directiva de protección del denunciante: un análisis desde el derecho público", *Revista General de Derecho Europeo*, n. 49, pp. 361-385 y Amoedo Barreiro, D., "Elementos esenciales para un sistema de protección del informante", *Revista Internacional de Transparencia e Integridad,* n. 4, 2017.

[51] En este sentido de recomendar la identificación del informante se han pronunciado la agencia francesa de protección de datos (CNIL, *Référentiel relatif aux traitements de données a caractère personnel destines a la mise en oeuvre d'un dispositif d'alertes professionnelles.* 18 juillet 2019, disponible en *https://www.cnil.fr/sites/default/files/atoms/files/referentiel-alertes-professionnelles_dec_2019.pdf),* así como el Supervisor Europeo de Protección de Datos (EDPS, *Guidelines on processing personal information within a whistleblowing procedure,* july 2016, disponible en https://edps.europa.eu/sites/default/files/publication/16-07-18_whistleblowing_guidelines_en.pdf). Con anterioridad a la aprobación de la Directiva, esta posición también la mantenían la agencia alemana (Federal Commissioner for Data Protection and Freedom of Information, *Annual Activity Report*

seriedad y fiabilidad de la información por parte de las autoridades; el cumplimiento de los plazos de acuse de recibo y de respuesta; la correcta gestión de la denuncia para la que puede requerirse más información a la persona informante y se facilita la investigación de las posibles denuncias falsas o realizadas de mala fe.

En relación con las denuncias maliciosas, tanto la Directiva como la Ley 2/2023 descartan la protección de las personas que actúen de mala fe, esto es, "quienes, en el momento de denunciar, comuniquen deliberada y conscientemente información incorrecta o engañosa" (Considerando 32) ni a quienes comuniquen información que ya esté completamente disponible para el público, rumores o habladurías no confirmados (Considerando 43). Al mismo tiempo, se garantiza que la protección no se pierda cuando el informante comunique información inexacta sobre infracciones por error cometido de buena fe.

Estos informantes de mala fe, además de no estar protegidos frente a posibles represalias, serán objeto de sanciones económicas [artículo 23.2 de la Directiva y artículo 63.1 *f)* de la Ley 2/2023] que también se pueden imponer a quien intente impedir la presentación de denuncias, a quienes adopten represalias contra los informantes y a quienes incumplan el deber de confidencialidad de la identidad del informante [artículo 23.1 de la Directiva y artículo 63.1 a), *b)* y *c)* de la Ley 2/2023].

En cualquier caso, debe subrayarse que las dificultades que pueda plantear la admisión de denuncias anónimas no pueden servir de excusa para rebajar las garantías que rodean a los informantes "que deben contar con el máximo amparo haciendo que prevalezca la denuncia, seria y circunstanciada, sobre cualquier otra actuación"[52], especialmente cuando la realidad ha demostrado en numerosas ocasiones la eficacia de esta vía que ha resultado decisiva para detectar irregularidades e incumplimientos graves. Una vez aceptada en la legislación nacional, cualquier complicación derivada de la presentación de una denuncia anónima puede superarse con una configuración y gestión adecuada del canal de denuncias que, entre otros, esté provisto "de las garantías de eficacia –de que se va a investigar igual que una denuncia no anónima– y de la posibilidad para el *whistleblower* de hacer un seguimiento y de conocer el desenlace de las alertas que ha efectuado"[53] así como del régimen de garantías y protección al informante anónimo que, posteriormente, se identifica para acogerse a ellas.

2005/2006, Disponible en https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/21TB_05_06.pdf?__blob=publicationFile&v=3) y danesa *(*Dutch DPA*, Whistle blowing-Opinion Dutch DPA,* january 2006, disponible en https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2004-1233_opinie_whblowing.pdf).

52 Vestri, G., "Aproximación al sistema de «whistleblowing». Un nuevo desafío para la Administración pública española". *Revista General de Derecho Administrativo*, n. 51, 2019, p. 51.

53 Sierra Rodríguez, J., "Anonimato y apertura de los canales de denuncia de la corrupción", *Revista General de Derecho Administrativo*, n. 55, 2020, p. 38.

IV. MEDIDAS PARA GARANTIZAR LA PROTECCIÓN DE LOS DATOS PERSONALES OBTENIDOS A TRAVÉS DE LOS CANALES DE DENUNCIAS

En España[54], hasta que no se aprobó la Ley de transposición de la Directiva, la regulación sobre canales de denuncia era escasa[52] y se concentraba en la establecida en la Ley 58/2003 General Tributaria (artículo 114); la Ley Orgánica 3/2007, de 22 de marzo para la igualdad efectiva de hombres y mujeres (artículo 48); la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (artículo 26 bis); el Código Penal tras su reforma en 2015 (artículo 31) y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (artículo 62).

Ninguna de las normas citadas menciona el sometimiento de todos los datos de carácter persona que pudieran contenerse en los canales de denuncia a la normativa de protección de datos. Tampoco se hacía referencia al tratamiento de datos personales en relación con los canales de denuncia en la Directiva 95/46/CE[56] ni en la LO 15/1999. En este sentido, se contaba únicamente con las mencionadas directrices del GT29 en su Dictamen 1/2006 y el criterio de la Agencia Española de Protección de Datos en su Informe 128/2007.

Frente a este vacío, el artículo 17 de la Directiva impone que todo tratamiento de datos personales realizado en aplicación de la misma se realizará de conformidad con el RGPD[57] y

---

54 Ante la ausencia de un órgano estatal, las Comunidades Autónomas han aprobado normativa para regular la implantación de canales de denuncias en el seno de sus respectivas administraciones y contamos con significativos ejemplos. Sin ánimo exhaustivo, pueden destacarse por su relevancia la Ley 14/2008, de 5 de noviembre, de la Oficina Antifraude de Cataluña; Ley de la Comunidad Valenciana 11/2016, de 28 de noviembre, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción; Ley de Castilla y León 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; Ley de las Islas Baleares 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Baleares; Ley de Aragón 5/2017, de 1 de junio, de Integridad y ética Públicas aprobada por las Cortes de Aragón; Ley 7/2018, de 17 de mayo, de creación de la Oficina de Buenas Prácticas y Anticorrupción de la Comunidad Foral de Navarra; Ley del Principado de Asturias 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés y Ley de Andalucía 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción. Un análisis de las leyes autonómicas encaminadas a combatir el fraude y la corrupción y a proteger al informante en Blanes Soliva, M. F. y Meco Tébar, F., "La protección de datos de las personas denunciantes en casos de corrupción en el sistema español", *cit*., pp. 153-185 y Tardío Pato, J. A., "La protección del denunciante para garantía del cumplimiento de la legalidad y evitar la corrupción", *Revista Española de Derecho Administrativo*, n. 217, 2022, pp. 29-33.

55 Fortuny Cendra, M. y Vilà Caselles, O., "Protección de los denunciantes y protección de datos", en *La Directiva de protección de los denunciantes y su aplicación práctica al sector público*, *cit.,* pp. 389 y ss.

56 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046

57 Más concretamente, la Directiva establece que todo tratamiento de datos tratamiento de datos personales, incluido el intercambio o la transmisión de datos personales por las autoridades competentes, debe efectuarse de conformidad con el RGPD y del Consejo y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. Todo intercambio o transmisión de información efectuado por las instituciones,

establece que los Estados miembros deben velar por que las autoridades competentes dispongan de procedimientos de protección adecuados para el tratamiento de las denuncias y para garantizar la protección de la identidad de cada informante, cada persona afectada y cada tercero que se mencione en la denuncia en todas las fases del procedimiento.

Asimismo, la Ley 2/2023 dispone que los tratamientos de datos personales deberán regirse por lo dispuesto en dicho Reglamento, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, destacadamente, por lo dispuesto en el artículo 24 LOPDGDD sobre "Sistemas de información de denuncias internas" cuya aplicación se amplía en la Ley 2/2023 a los canales de denuncias externos[58].

1. Los principios de tratamiento de datos personales aplicados a los canales de denuncia

La Directiva hace especial hincapié en la aplicación de los principios de tratamiento de los datos que enumera el artículo 5 RGPD. Se trata de principios nucleares en la configuración del canal de denuncias y cuya concreción se determina en el mencionado artículo 24 LOPGDD, concretamente:

a) **Principios de licitud, lealtad y transparencia:** aplicados al canal de denuncias se traducen en el deber de informar a empleados y terceros sobre la existencia de los sistemas de información de denuncias y sobre el tratamiento de datos. La simple advertencia no satisface esta exigencia sino que se ha de informar sobre la existencia, objetivo y funcionamiento del sistema, los destinatarios de la información y derechos de las personas afectadas y el mantenimiento de la confidencialidad de la identidad del informante y de los destinatarios.

b) **Principio de limitación de la finalidad:** el tratamiento de los datos que se realice en la gestión del canal de denuncias debe responder a la finalidad del mismo que es determinar si se han cometido irregularidades o ilícitos, por tanto, los datos personales servirán a la gestión del registro de la denuncia, el análisis y resolución de la misma.

c) **Principio de minimización de datos:** habida cuenta de que los datos a tratar han de ser los referidos exclusivamente a los hechos denunciados, el cumplimiento de este principio está muy relacionado con el modo como se presente la denuncia que ha

---

órganos u organismos de la Unión debe llevarse a cabo de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.

[58] El contenido del artículo 24 LOPDGDD se modifica a partir de lo dispuesto en la Disposición final séptima de la Ley 2/2023 la cual se considerará, tras su promulgación, como legislación específica en relación al tratamiento de datos personales relativo a los sistemas de información internos y externos sobre posibles infracciones normativas y de lucha contra la corrupción que, en todo caso, estarán sujetas a lo estipulado en la normativa vigente en materia de protección de datos (RGPD y LOPDGDD).

de determinar con la mayor claridad posible esos hechos. La exactitud en esta determinación impedirá que se traten otros datos que sean irrelevantes o excesivos, incluso categorías especiales de datos al referirse a ideología, religión, afiliación sindical, creencias, salud, origen racial u étnico, vida sexual, datos genéticos y biométricos, así como datos relativos a condenas e infracciones penales.

d) **Principio de limitación del plazo de conservación:** todos los sujetos obligados a disponer de un canal interno de informaciones deberán contar con el libro-registro de las comunicaciones recibidas y de las investigaciones internas en que hubieran derivado las anteriores. Según la Directiva, los datos personales relativos a esas comunicaciones e investigaciones se conservarán durante el plazo de tiempo estrictamente necesario y proporcionado para dar cumplimiento a la finalidad de investigación para la cual fueron recopilados. La Ley 2/2023 concreta que dicho plazo de conservación no puede exceder, en ningún caso, de diez años desde que fueran objeto de tratamiento para los fines referidos.

Por su parte, transcurridos tres meses desde la recepción de la comunicación sin que se hubieran iniciado actuaciones de investigación, se procederá a la supresión de tales datos, salvo que la finalidad de su conservación fuera dejar evidencia del funcionamiento del sistema, en cuyo caso el contenido de las comunicaciones constará de manera anonimizada. Además, se autoriza la conservación anonimizada de las denuncias a las que no se haya dado curso.

e) **Principios de integridad y confidencialidad:** las garantías de ambos principios se llevan a cabo mediante el análisis de riesgos inherentes al tratamiento de datos del canal de denuncias y una evaluación de impacto en caso de identificarse un riesgo alto para los derechos y libertades de las personas.

   La preservación de la identidad del informante, para protección suya y de terceras personas, permite restringir mediante ley el ejercicio de determinados derechos de protección de datos de las personas afectadas como, por ejemplo, el derecho de acceso.

   También ha de limitarse el acceso a los datos del sistema de información a las personas responsables de las funciones de control y cumplimiento que pueden ser de la propia organización o externos y a los posibles encargados de tratamiento.

f) **Principio de responsabilidad proactiva:** consiste en la aplicación de medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento es conforme con el RGPD y que se concretan, entre otras, en la protección de datos desde el diseño y por defecto, registro de actividades de tratamiento, política de privacidad del canal de denuncias, protocolo de actuación ante brechas de seguridad, evaluación de riesgo y de impacto del tratamiento de datos[59].

[59] Fortuny y Vilà completan este listado con los siguientes protocolos: protocolo de atención de derechos, protocolo de retención de datos personales en relación con el sistema de denuncias, protocolo de protección de datos desde el diseño y por defecto, protocolo que estipule las medidas de seguridad adecuadas para el sistema y que garantice la confidencialidad en el mismo y protocolo de contratación de

2. Requisitos para la configuración de los canales de denuncia en la Ley 2/2023 de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción

Estos principios o directrices que guían el tratamiento de los datos personales en la gestión del canal de denuncias completan el deber esencial de confidencialidad al que se refiere la Directiva en su Considerando 82, en relación con el artículo 16, donde expone que "Una medida ex ante esencial para evitar represalias consiste en salvaguardar la confidencialidad de la identidad del informante durante el proceso de denuncia y las investigaciones desencadenadas por la denuncia". Este deber de confidencialidad asegura la inmunidad de la persona informante, lo que implica el mantenimiento de su identidad reservada, y en torno a él se diseñan las características del tratamiento de datos en los canales de denuncia (legitimación, restricción de derechos personalísimos, medidas organizativas, obligación de información, etc.).

Centrándonos en la Ley 2/2023[60] y por lo que respecta a la base de legitimación del tratamiento de datos objeto de regulación cabe destacar que, si la existencia de un sistema de información interno y/o externo responde a una obligación conforme a lo estipulado en la Directiva, la licitud de dicho tratamiento se fundamenta en el cumplimiento de una obligación legal [artículo 6.1.c) RGPD]; en cambio, cuando el tratamiento de tales datos personales tenga carácter voluntario o se lleve a cabo en el ámbito de la revelación pública, dicho tratamiento se considerará lícito en base a su necesidad para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de dicho tratamiento [artículo 6.1.e) RGPD].

En este segundo supuesto, el responsable del tratamiento de los datos personales lleva a cabo el mismo a partir de la existencia de un "motivo legítimo imperioso" (artículo 21.1 RGPD), lo que faculta la restricción del ejercicio de determinados derechos personalísimos en materia de protección de datos de las personas objeto de investigación durante el tiempo necesario para evitar las obstaculizaciones o retrasos en las investigaciones[61].

Concretamente, el responsable de dicho tratamiento no estará obligado a dejar de tratar tales datos personales del interesado por el mero ejercicio, por parte de este último, de su derecho de oposición en materia de protección de datos[62]. También puede verse

---

proveedores vinculados al sistema de denuncias (Fortuny Cendra, M. y Vilà Caselles, O., "Protección de los denunciantes y protección de datos", *cit.,* pp. 417 y 418).

60 Un completo análisis de las previsiones contenidas en el Título VI del que fuera Proyecto de Ley sobre la aplicación de la protección de datos personales al canal de denuncias, que mantiene su actualidad ante la redacción definitiva de la Ley 2/2023, en Puyol Montero, J., "La protección de Datos en el ámbito del Canal de Denuncia. Especial consideración al Anteproyecto de Ley de Trasposición de la Directiva de Alertadores", *La Ley Privacidad*, n. 12, 2022.

61 Nos referimos al derecho que asiste al denunciado a ejercer los derechos de acceso, rectificación, cancelación u oposición ninguno de los cuales "podrá desconocerse pero sí modular su efectividad ajustándose a la naturaleza, alcance y finalidad del sistema interno de denuncia" (Rallo Lombarte, A., "Whistleblowing (sistemas internos de denuncias) y protección de datos", *cit.,* p. 109).

62 El artículo 31 de la Ley 2/2023 determina que "4. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición

limitado el derecho de acceso a los datos personales de la persona informante para garantizar la protección de esta frente a posibles represalias por parte de las personas investigadas por la información suministrada y salvaguardar su libertad de actuación en beneficio del buen gobierno empresarial.

En cuanto a las personas legitimadas a las que se les aplicará la normativa transpuesta serán las personas informantes que trabajen en el sector público o privado y que hayan obtenido información sobre infracciones en un contexto laboral o profesional. Estos informantes estarán cubiertos por la protección vinculada específicamente a la normativa sobre protección de datos personales y las garantías derivadas de la regulación contenida sobre esta materia en la Ley 2/2023[63].

Por su parte, a los informantes y a todas aquellas personas que hagan uso del canal de revelación pública, se les informará de que, con motivo de su comunicación, su identidad se mantendrá reservada, no revelándose a ningún tercero no autorizado, incluyendo la persona sobre la que versan supuestamente tales hechos, ninguna información relativa a los hechos comunicados ni aquellos otros a través de los que se pudiera identificar su persona; si bien, ello no exime de la necesidad de garantizar los derechos en materia de protección de datos (artículos 15 a 22 RGPD) de todos los interesados afectados por dicho tratamiento de datos personales, con las limitaciones anteriormente indicadas.

Así, la comunicación de los datos de la persona informante solo podrá hacerse a determinadas entidades, tales como la Autoridad judicial, el Ministerio fiscal o la Autoridad administrativa con competencia que corresponda (artículo 33.3 de la Ley 2/2023). No obstante, será lícito "el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan" (artículo 32.2 de la Ley 2/2023).

Si los datos contenidos en los sistemas de denuncias se tuvieran que transmitir a una tercera compañía a cargo de la investigación del hecho denunciado también se producirá una comunicación de datos de la que hay que informar tanto al informante como al denunciado. La misma situación y obligación de informar se dará ante una posible transferencia internacional de datos a otras empresas del grupo.

Por su parte, el acceso a los datos personales contenidos en los sistemas de información internos se limita a las siguientes figuras responsables:

a) responsable del sistema y quien lo gestione directamente;

b) el responsable u órgano público competente de la gestión de los recursos humanos en relación a un procedimiento disciplinario;

c) el responsable de los servicios legales de la entidad, en el caso del inicio de acciones legales que correspondan;

---

se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales".

63 Puyol Montero, J., "La protección de Datos en el ámbito del Canal de Denuncia. Especial consideración al Anteproyecto de Ley de Trasposición de la Directiva de Alertadores", *cit.*

d) los encargados del tratamiento designados a tal respecto; y

e) el delegado de protección de datos.

En relación con esta última figura, todas las entidades obligadas a configurar un sistema de información interno, los terceros encargados de dicha gestión, la Autoridad independiente de protección de datos que corresponda y las autoridades independientes de protección del informante que a tal efecto se constituyesen, estarán obligados a designar un Delegado de Protección de Datos, para promover el cumplimiento normativo en materia de protección de datos durante todo el proceso de gestión de la información y preservar así el derecho a la protección de datos de todas las personas físicas que pudieran verse afectadas por el mismo.

Finalmente, además de estas previsiones normativas sobre el tratamiento de datos en los canales de denuncias, debe atenderse a las recomendaciones de la Agencia Española de Protección de Datos sobre "Privacidad en sistemas de denuncias o whistleblowing"[64].

V. CONCLUSIÓN

Una adecuada protección de las personas informantes es esencial para la salvaguardia del interés público, proteger la libertad de expresión y promover la transparencia y rendición de cuentas. La aprobación de la Directiva (UE) 2019/1937 ha facilitado un mínimo común regulador para los Estados miembros que, hasta entonces, contaban con normativas muy heterogéneas y de diverso alcance. España, si bien con retraso, ha transpuesto la Directiva que cuenta con algunas novedades positivas al elevar la protección del informante haciendo uso del margen de maniobra nacional que permite la Directiva. Concretamente, la Ley 2/2023 amplía su ámbito de aplicación al proteger a quienes informen sobre las infracciones de Derecho de la Unión, como marca la Directiva, sino también a quienes adviertan de las infracciones penales y administrativas graves y muy graves de nuestro ordenamiento jurídico; asimismo, en el ámbito privado y con independencia del número de empleados, obliga a contar con un sistema interno de información a partidos políticos, sindicatos, patronales y fundaciones siempre que reciban o gestionen fondos públicos y, muy especialmente, la aceptación explícita de las denuncias anónimas que la Directiva permite pero no potencia.

Uno de los elementos nucleares del régimen de inmunidad de las personas informantes es la protección de sus datos de carácter personal de forma que los canales de denuncias se gestionen con absoluta observancia de la normativa de protección de datos. El derecho a la protección de datos de carácter personal también ha de garantizarse a las personas denunciadas por su vinculación con otros derechos como la presunción de inocencia, la intimidad o el honor. La Directiva y la Ley 2/2023 mantienen un delicado equilibrio entre los derechos de las personas informantes y las personas afectadas, tratando de promover

[64] Agencia Española de Protección de Datos, *Privacidad en sistemas de denuncias o 'whistleblowing'*, 14 de octubre de 2021, https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-en-sistemas-de-denuncia-o-whistleblowing

las denuncias, pero al mismo tiempo atajando las denuncias falsas o malintencionadas y previniendo daños reputacionales injustificados.

Por otra parte, el tratamiento ilícito de los datos de carácter personal en el seno de cualquier organización o institución pública o privada puede dar lugar a una denuncia por incumplimiento de la normativa europea —y nacional—. De modo que existe una doble faceta de la protección de datos personales en los sistemas de cumplimiento normativo (*compliance*) a los que estos canales sirven como herramienta esencial.

A lo largo de nuestro trabajo hemos analizado la protección de los informantes desde el punto de vista de la protección de datos tanto en la Directiva como en la Ley 2/2023 que la transpone. Destacamos las siguientes ideas clave:

- El interés público se erige como condición para que las personas informantes puedan acceder a protección. Esto descarta las quejas de carácter subjetivo y personal y protege frente a denuncias abusivas o maliciosas.
- La prelación de vías para la comunicación o denuncia (canal interno, canal externo o revelación pública) ofrece una cobertura completa, aunque en el caso de las denuncias anónimas existe un consenso sobre las mayores dificultades de protección al informante y la revelación pública está sometida a ciertas condiciones.
- Tanto los canales internos como externos han de diseñarse, construirse y gestionarse con seguridad para garantizar la confidencialidad y ser capaces de almacenar la información para permitir futuras investigaciones. La pieza clave en el estatus de inmunidad que rodea a la persona informante para protegerla frente a represalias se construye sobre la confidencialidad en el tratamiento de su identidad y demás datos personales que no podrán revelarse salvo obligación legal en el contexto de investigaciones judiciales.
- También respecto de la persona denunciada y terceras partes se exige el mantenimiento de todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia; en fin, de los mismos derechos que goza el informante.
- En el diseño de los canales de denuncia es importante la aplicación de los principios de privacidad desde el diseño y por defecto para garantizar la calidad de los datos y minimización de los datos, esto es, que no se traten más datos personales que los estrictamente necesarios.
- Las organizaciones deben proporcionar información clara, accesible e identificables sobre las condiciones para acogerse a la protección del informante en virtud de la Directiva.
- El periodo de conservación de los informes ha de ser el estrictamente necesario para realizar la investigación y limitado para aquellos informes que no han conducido a la apertura de una investigación.
- Dado que la información tratada es sensible y en atención a las consecuencias adversas que filtraciones o revelaciones no autorizadas pudieran tener tanto para los informantes como para los denunciados, se debe tener especial cuidado con las

medidas técnicas y organizativas necesarias para mitigar los riesgos y garantizar la seguridad de los datos. La singularidad material de estos sistemas internos de denuncias hace recomendable la especialización de los medios humanos y materiales utilizados para la gestión de las denuncias diferenciándolos del resto de recursos técnicos, humanos y materiales de la entidad para reducir los riesgos de accesos indebidos al sistema de denuncias[65].

Finalmente, destacamos que la Directiva impone a los Estados miembros la presentación de un informe de ejecución y aplicación de la Directiva dos años después del término de transposición (17 de diciembre de 2023) y la Comisión, a su vez, a los cinco años (17 de diciembre de 2025) presentará un informe al Parlamento Europeo y al Consejo en el que evaluará evaluando la eficacia, eficiencia y coherencia global de las normas nacionales de transposición. Será la oportunidad de evaluar si son necesarias medidas adicionales o modificaciones con vistas a la mejora de la protección de los informantes y del entorno laboral para proteger la salud, la seguridad y las condiciones de trabajo de los trabajadores.

[65] Rallo Lombarte, A., "Whistleblowing (sistemas internos de denuncias) y protección de datos", *cit.,* p. 111.