Comentario a la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción

El pasado 21 de febrero de 2023 se publicó en el *Boletín Oficial del Estado* la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción ("Ley 2/2023"). El nuevo texto, que entrará en vigor el próximo 13 de marzo de 2023, responde a la obligación impuesta al legislador español de transponer la Directiva 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 ("Directiva de Whistleblowing").

1. ASPECTOS PRINCIPALES

La Ley 2/2023, que transpone al ordenamiento jurídico español la Directiva de Whistleblowing, pretende reforzar la cultura de cumplimiento de las entidades públicas y privadas mediante la protección de los denunciantes que informen sobre infracciones conocidas en el contexto laboral o profesional. En este sentido, las principales novedades que introduce esta norma son las siguientes:

(i) Amplía el **ámbito de aplicación** de la Directiva de Whistleblowing respecto del tipo de comunicaciones que generan el derecho de protección.

(ii) Obliga a implementar **canales internos de información** a las entidades públicas y a las privadas de 50 o más trabajadores (entre otras), que deberán cumplir determinadas características y garantías mínimas.

(iii) Requiere la **tramitación efectiva** de las comunicaciones, en la que también habrá que respetar una serie de garantías y derechos mínimos.

(iv) Se exige la **integración de todos los canales** de las entidades en un único sistema interno de información, garantizando así que la recepción y tramitación de todas las comunicaciones sobre potenciales infracciones cumplan las exigencias de la Ley 2/2023.

(v) Se exige que las entidades admitan y tramiten **denuncias anónimas**.

(vi) Dispone la creación de la **Autoridad Independiente de Protección al Informante**, con potestades sancionadoras en esta materia y con responsabilidades de gestión del canal externo de denuncias que también crea la ley, así como de las medidas de apoyo a los informantes, entre otras funciones.

(vii) Legitima la **revelación pública** de las infracciones en determinados supuestos.

(viii) Impone la **obligación al órgano de administración** o de gobierno de **designar a un responsable** del sistema de información interno.

(ix) Las **medidas de protección** no se limitan exclusivamente a la prohibición de represalias, sino también a medidas de tipo asistencial, que en algunos casos pueden incluso implicar la concesión de apoyo financiero al informante.

A continuación, se da respuesta de forma sintetizada a las principales preguntas que cabe formular al hilo de la nueva regulación, poniendo especialmente el foco en las obligaciones que afectan a las empresas privadas en relación con la implantación de sistemas internos de información[1].

2. ¿A QUÉ TIPO DE COMUNICACIONES SE APLICA?

El ámbito objetivo de la norma comprende todas las comunicaciones que versen sobre:

- **infracciones del Derecho de la Unión Europea** cuando (i) afecten a alguna de las materias señaladas en el Anexo I de la Directiva de Whistleblowing, (ii) afecten a los intereses financieros de la Unión o (iii) incidan en el mercado interior;
- **infracciones administrativas** graves o muy graves; o
- **hechos delictivos**.

Se contemplan algunas excepciones, como por ejemplo las comunicaciones relativas a información clasificada o que puedan afectar a la seguridad del Estado, que no entrarían en el ámbito de protección de la norma.

3. ¿A QUIÉN PROTEGE LA LEY?

A cualquier persona que en un **contexto laboral o profesional** haya obtenido información sobre presuntas infracciones, ya sea en el sector público o en el privado. La protección no se circunscribe a los empleados de los sujetos obligados, sino también a cualquier otra persona que, en el ejercicio profesional o en el marco de la prestación de servicios, haya interactuado con dichos sujetos. La Ley 2/2023 incluye el siguiente listado no exhaustivo:

- empleados públicos;
- trabajadores por cuenta ajena;

[1] Nótese que este documento no analiza al detalle todas las materias reguladas por la Ley 2/2023, sino que se centra en explicar de forma general sus aspectos principales.

- autónomos;
- accionistas, miembros del órgano de administración, dirección o supervisión de una entidad;
- voluntarios, becarios y trabajadores en períodos de formación; y
- cualquier persona que trabaje para contratistas, subcontratistas y proveedores.

Las comunicaciones pueden referirse a hechos conocidos en el ámbito de una relación laboral o profesional (i) todavía en vigor, (ii) ya finalizada o (iii) incluso no iniciada (por ejemplo, si se refiere a infracciones relativas a procesos de selección o de negociación precontractual).

El alcance de la protección se extiende a las **personas relacionadas con el informante** (compañeros de trabajo, familiares, personas jurídicas para las que trabaje o de las que sea titular, etc.). Asimismo, se extenderá a toda persona física que haya asistido al informante y, específicamente, a los representantes legales de los trabajadores en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

4. ¿QUIÉN DEBERÁ IMPLEMENTAR UN SISTEMA INTERNO DE INFORMACIÓN?

La obligación de disponer de un sistema interno de información se prevé tanto para las entidades públicas como para las privadas que se indican a continuación:

ÁMBITO PÚBLICO	ÁMBITO PRIVADO
• Administraciones estatales, autonómicas y locales, así como sus organismos o entidades dependientes. • Autoridades administrativas independientes (Banco de España, Seguridad Social, etc.). • Universidades públicas. • Corporaciones de Derecho Público. • Fundaciones del sector público. • Sociedades mercantiles participadas mayoritariamente por alguna de las entidades enumeradas anteriormente. • Órganos constitucionales, de relevancia constitucional o análogos autonómicos.	• Personas físicas o jurídicas que tengan contratados a 50 o más trabajadores. • Personas jurídicas que entren en el ámbito de aplicación del Derecho comunitario en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales y financiación del terrorismo, seguridad del transporte o protección del medio ambiente. • Partidos políticos, sindicatos, así como las organizaciones empresariales y fundaciones creadas por ellos que reciban fondos públicos.

En los **grupos de empresas**, la sociedad dominante (i) aprobará una política general relativa al sistema interno de información y a la defensa del informante y (ii) se asegurará de la aplicación de sus principios por todas las sociedades que conformen el grupo, sin perjuicio de la independencia y autonomía de cada sociedad en función del sistema de gobierno corporativo del grupo del que se trate y de las modificaciones o adaptaciones que fueran necesarias para el cumplimiento de la normativa que les resulte aplicable.

Las **entidades de menor tamaño** (entre 50 y 249 trabajadores) podrán compartir entre sí el sistema interno de información y los recursos destinados a la tramitación de las comunicaciones, respetando en todo caso las garantías previstas en la ley.

El **plazo máximo de implementación** de los sistemas internos de información será de 3 meses a partir de la entrada en vigor de la ley (i. e., hasta el 13 de junio de 2023). Excepcionalmente, las entidades con menos de 250 empleados tendrán hasta el 1 de diciembre de 2023 para cumplir con la normativa.

5. ¿QUÉ PERSONAS SON RESPONSABLES DE LA IMPLEMENTACIÓN Y GESTIÓN DEL SISTEMA?

En lo que se refiere a la implementación, la responsabilidad recae en el **órgano de administración** o de gobierno de cada entidad, que deberá seguir un trámite de consulta con los representantes legales de los trabajadores a tal efecto y tendrá la condición de responsable del tratamiento de los datos personales del sistema interno de información.

En lo que respecta a la gestión del sistema y la tramitación de las comunicaciones, las entidades deberán contar con un **responsable del sistema interno de información**, que deberá cumplir los siguientes requisitos:

- Ser específicamente designado por el órgano de administración o de gobierno.
- En caso de tratarse de un órgano colegiado, este deberá delegar en uno de sus miembros la gestión del sistema y la tramitación de los expedientes de investigación.
- Deberá gozar de plena independencia y autonomía respecto del resto de los órganos de la entidad (incluyendo el órgano de administración).
- En el sector privado, deberá ser un directivo de la entidad que asumirá exclusivamente esas funciones (salvo que no estuviera justificado), si bien podrá coincidir en la persona responsable de la función de cumplimiento normativo.
- El nombramiento o el cese deberá ser notificado a la Autoridad Independiente de Protección del Informante en el plazo de los 10 días hábiles siguientes.

6. ¿QUÉ REQUISITOS DEBE REUNIR EL SISTEMA INTERNO DE INFORMACIÓN?

El sistema interno de información constituirá el **cauce preferente** para la comunicación y tramitación de denuncias (frente al canal externo o la revelación pública).

Los **principios esenciales** del sistema interno de información pueden sintetizarse en los siguientes:

- Garantía de confidencialidad de la identidad del informante y de cualquier tercero mencionado, así como del tratamiento de la información y su investigación.
- Garantías frente a la adopción de represalias.
- Respeto al principio de presunción de inocencia y derecho de defensa de las partes afectadas.
- Garantía de independencia, imparcialidad y ausencia de conflictos de interés.
- Tramitación efectiva de las comunicaciones.

Asimismo, la Ley 2/2023 exige a los sujetos obligados la **integración de todos los canales internos** operativos en la entidad para la denuncia de posibles infracciones (tales como, por ejemplo, canales de prevención del acoso, de la prevención de delitos o infracciones del código ético de la entidad, etc.).

Adicionalmente, las entidades estarán obligadas a disponer de (i) una **política** que enuncie los principios generales del sistema y (ii) un **procedimiento de gestión de comunicaciones**, que deberá ser aprobado por el órgano de administración o de gobierno y de cuya efectiva implementación responderá el responsable del sistema interno de información. El procedimiento de gestión deberá contener, al menos, la siguiente información:

a) Relación de los canales internos disponibles.

b) Información clara y accesible sobre canales externos de información y ante las instituciones u organismos de la Unión Europea.

c) Obligación de acusar recibo al informante y fijación de un plazo máximo para dar respuesta a las comunicaciones recibidas.

d) Posibilidad de mantener una vía de comunicación con el informante y de solicitarle información adicional.

e) Derechos de la persona denunciada (a que se le informe de las infracciones que se le atribuyen, a ser oída en cualquier momento, al honor, etc.).

f) Extensión de la garantía de confidencialidad respecto de las comunicaciones que se cursen a través de canales o personas distintas de las previstas en el sistema, debiendo formarse expresamente al personal en esta materia.

g) Exigencias derivadas del cumplimiento de la normativa sobre protección de datos personales.

h) Obligación de remitir la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito y a la Fiscalía Europea cuando afecten a los intereses financieros de la Unión. Esta referencia a la remisión de información al Ministerio Fiscal no venía exigida por la Directiva de Whistleblowing y entendemos que no debe interpretarse en el sentido de que la persona jurídica carece del derecho a defenderse o a no confesarse culpable, según resulte de aplicación.

7. ¿CÓMO DEBERÁN FORMULARSE LAS COMUNICACIONES?

El sistema de información contará con un canal interno para la gestión de las comunicaciones, con la **posibilidad de externalizarlo** a través de un tercero, que deberá ofrecer garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones, y que tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. En todo caso, la gestión por un tercero externo no podrá suponer un traslado de las obligaciones atribuidas al responsable del sistema en persona distinta.

En cuanto a la **presentación de las comunicaciones**, el sistema interno de información deberá permitir su presentación de forma verbal o escrita (o por ambas):

- En lo que respecta a comunicaciones verbales, estas podrán formularse por vía telefónica o por sistema de mensaje de voz. Además, previo consentimiento del informante, las denuncias verbales deberán documentarse mediante una grabación o transcripción, ofreciendo al informante la posibilidad de revisarla y firmarla en este último supuesto.
- En lo que se refiere a las comunicaciones por escrito, estas se podrán remitir por correo postal o por cualquier medio electrónico habilitado al efecto.

Si lo solicita el informante, deberá darse la posibilidad de agendar una reunión presencial. Asimismo, el informante podrá señalar el modo en el que prefiere recibir las notificaciones relativas al tratamiento de la comunicación, indicando un domicilio, un correo electrónico o un lugar seguro a tal efecto.

El canal interno de información deberá permitir la presentación de **denuncias anónimas**, cuestión que la Directiva de Whistleblowing había dejado a elección de cada uno de los Estados miembros.

8. ¿CUÁL ES EL RÉGIMEN DE PUBLICIDAD Y REGISTRO?

Las entidades que cuenten con una **página web** deberán incluir en su página de inicio (en una sección separada y fácilmente identificable) información clara y accesible sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión.

De igual manera, los sujetos obligados deberán disponer de un **libro-registro** de las comunicaciones recibidas y las de investigaciones realizadas. Dicho registro no será público y únicamente podrán acceder a él los jueces y tribunales en el marco de un procedimiento judicial. Los datos personales relacionados con las comunicaciones e investigaciones únicamente se conservarán durante el período que fuese necesario, que en ningún caso podrá superar los diez años.

9. ¿QUÉ PLAZOS NUEVOS HAY QUE TENER EN CUENTA?

En caso de que el informante solicite mantener una **reunión presencial**, la entidad deberá fijarla dentro del plazo máximo de siete días desde la formulación de la petición.

Tras la recepción de la comunicación, la entidad deberá enviar **acuse de recibo** al informante en el plazo máximo de siete días.

El **plazo máximo para dar respuesta** a las actuaciones de investigación se establece en tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requirieran una ampliación del plazo, en cuyo caso este podrá extenderse hasta un máximo de otros tres meses adicionales.

La norma establece también determinados plazos que deben cumplirse en materia de conservación y eliminación de **datos personales**. Estos plazos están en línea con los previstos hasta ahora en la normativa previa de protección de datos. En particular, se establece que las comunicaciones podrán

mantenerse dentro del sistema de información únicamente durante el tiempo imprescindible para decidir sobre si procede o no iniciar una investigación. Si esta decisión no se adoptara en un plazo de tres meses, deberá suprimirse del sistema la comunicación, salvo con el fin de mantener evidencia del funcionamiento del sistema y de forma anonimizada si fueran comunicaciones no cursadas. Por tanto, los sistemas deben diseñarse e implementarse de una forma adecuada para cumplir con estas obligaciones de supresión.

10. ¿QUÉ IMPLICA LA PROHIBICIÓN DE REPRESALIAS?

La **prohibición de represalias** (concepto amplio que comprende *"cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable"*) incluye la propia tentativa o amenaza de represalia. Uno de los principales efectos de esta prohibición es que, en el marco de procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, se establece la presunción de que dichos perjuicios constituyen una represalia por haber comunicado la información. De este modo, aquel que haya adoptado la medida supuestamente perjudicial deberá probar que se basó en circunstancias ajenas a la comunicación y que estaba debidamente justificada. Dicho de otro modo, se introduce una **inversión de la carga de la prueba** en esta materia. Otros ejemplos de implicaciones derivadas de la prohibición de represalias es el **carácter nulo de pleno derecho de los actos administrativos** que tengan por objeto impedir o dificultar la presentación de comunicaciones o que constituyan represalias, así como la posibilidad de aplicar **medidas disciplinarias** correctoras o de reclamar la correspondiente **indemnización de daños y perjuicios**.

Asimismo, se establecen otras **medidas de protección** de diversa naturaleza, incluyendo de tipo asistencial (asesoramiento e información, asistencia jurídica, apoyo financiero, apoyo psicológico, etc.), a cargo de la Autoridad Independiente de Protección.

11. ¿QUÉ REGLAS SE ESTABLECEN PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN?

La Ley 2/2023 regula de forma detallada cómo deben tratarse los datos personales de los informantes y demás personas involucradas en una comunicación e investigación posterior y deroga expresamente la regulación previa de esta materia contenida en la normativa de protección de datos. Las reglas previstas en la Ley 2/2023 abarcan desde la fijación de las bases que legitiman estos tratamientos de datos, hasta cuáles son las principales reglas para minimizar el tratamiento en estos sistemas (p.ej., listando de forma exhaustiva qué perfiles dentro de las empresas pueden acceder a los datos contenidos en el sistema de información). Otro de los aspectos que destacan es la obligación de las empresas de preservar la identidad de la persona que presente la comunicación, a la que se le reconoce el derecho a que no se haga pública su identidad.

12. ¿QUÉ SANCIONES SE PREVÉN PARA INFRACCIONES MUY GRAVES?

En caso de incumplimiento o implementación deficiente de los sistemas de información, las entidades podrían enfrentarse a **sanciones** que, en caso de infracciones muy graves, podrían alcanzar:

- Multas de hasta 1.000.000 de euros para las personas jurídicas y 300.000 euros para las personas físicas.
- Amonestaciones públicas.
- Prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo de 4 años.
- Prohibición de contratar con el sector público durante un plazo de 3 años.

Las sanciones por infracciones muy graves de cuantía igual o superior a 600.001 euros impuestas a personas jurídicas podrían ser publicadas en el *Boletín Oficial del Estado* tras la firmeza de la resolución en vía administrativa. Asimismo, y puesto que la norma recoge una serie de reglas específicas en materia de protección de datos personales, el incumplimiento de estas podría dar lugar a sanciones administrativas bajo el Reglamento General de Protección de Datos[2].

[2] Reglamento (U) 679/2016 General de Protección de Datos.

URÍA
MENÉNDEZ

13. ABOGADOS DE CONTACTO

Enrique Rodríguez Celada
Counsel - PENAL
+34915860550
enrique.rodriguez@uria.com

Mario Barros
Socio - LABORAL
+34915864554
mario.barros@uria.com

Leticia López-Lapuente
Socia - PROTECCIÓN DE DATOS
+34915860131
leticia.lopez-lapuente@uria.com