

LA NUEVA LEY DEL INFORMANTE Y SU REPERCUSIÓN EN EL ÁMBITO PENAL

Guillermo GARCÍA-PANASCO MORALES

Fiscal

Doctor en Derecho

Letrado del Tribunal Constitucional

ggarciapanasco@tribunalconstitucional.es

RESUMEN

El objeto de este trabajo es analizar las consecuencias que la entrada en vigor de la Ley 2/2023, de 20 de febrero, conocida como la «Ley del informante», puede tener en determinados ámbitos del Derecho penal y procesal penal. En particular, se abordará la repercusión del nuevo sistema de información en la configuración de la responsabilidad penal de las personas jurídicas y, singularmente, en el contenido y eficacia de los programas de compliance. Seguidamente, se analizarán diversos problemas prácticos como el contenido de las investigaciones internas y la posible afectación de algunos derechos fundamentales (mediante el registro de dispositivos electrónicos o la utilización de grabaciones de seguridad), con especial atención a las garantías derivadas de la necesaria protección de los derechos a la defensa y a la presunción de inocencia de las personas físicas y jurídicas, para que las diligencias practicadas puedan ser utilizadas en un proceso penal.

Palabras clave: Whistleblowing, informante, denuncia, compliance, Derecho penal, ne bis in idem.

ABSTRACT

The purpose of this piece of work is to look into the impact that the entry into force of Law 2/2023, of February 20 or «Informer Law», may have on certain areas of criminal law and criminal procedures. Particularly, the impact of the new information system on the configuration of the criminal liability of legal entities and, singularly, on the content and effectiveness of compliance programs will be addressed. Next, various practical problems will be looked upon, such as the content of internal investigations and the possible impact of some fundamental rights (through the registration of electronic devices or the use of security recordings), with special attention to the guarantees derived from the necessary protection of the rights to defense and to the presumption of innocence of natural and legal persons, so that the proceedings carried out can be used in a penal procedure.

Keywords: Whistleblowing, whistleblower, complaint, compliance, Criminal Law, ne bis in idem.

ZUSAMMENFASSUNG

Ziel dieser Arbeit ist es, die Folgen zu analysieren, die das Inkrafttreten des Gesetzes 2/2023 vom 20. Februar, bekannt als das «Hinweisbergesetz», auf bestimmte Bereiche des Strafrechts und des Strafverfahrens haben kann. Insbesondere werden die Auswirkungen des neuen Informationssystems auf die Ausgestaltung der strafrechtlichen Verantwortlichkeit von juristischen Personen und insbesondere auf den Inhalt und die Wirksamkeit von Compliance-Programmen behandelt. Anschließend werden verschiedene praktische Probleme analysiert, wie der Inhalt interner Ermittlungen und die möglichen Auswirkungen auf bestimmte Grundrechte (durch die Durchsuchung elektronischer Geräte oder die Verwendung von Sicherheitsaufzeichnungen), mit besonderem Augenmerk auf die Garantien, die sich aus dem notwendigen Schutz der Verteidigungsrechte und der Unschuldsvermutung natürlicher und juristischer Personen ergeben, damit die durchgeführten Verfahren in Strafverfahren verwendet werden können.

Schlüsselwörter: Whistleblowing, Hinweisgeber, Meldung, Compliance, Strafrecht, *ne bis in idem*.

SUMARIO: I. INTRODUCCIÓN.—II. EL NUEVO SISTEMA DE INFORMACIÓN Y LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS.—1. Los programas de *compliance*.—2. El rol del *compliance officer*.—3. La eventual concurrencia de un *bis in idem*.—III. EL NUEVO SISTEMA DE INFORMACIÓN Y SU POSIBLE EFECTO EN EL PROCESO PENAL.—1. El concepto de denunciante y su necesaria contextualización.—2. Los derechos y obligaciones de las partes implicadas y su eventual repercusión para la persona jurídica.—3. El contenido de la investigación: algunos supuestos problemáticos.—3.1. El análisis de los dispositivos electrónicos puestos a disposición de los trabajadores (la doctrina Barbulescu).—3.2. El análisis de los sistemas de grabación (la doctrina López Ribalda).—*a*) Sobre el derecho a la protección de datos.—*b*) Sobre el derecho a la intimidad.—4. Los derechos y las garantías en la investigación de hechos con relevancia penal.—IV. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El pasado 13 de marzo de 2023 entró en vigor 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 corrupción¹ (en adelante, Ley 2/2023 o Ley del informante) por la que se transpone a nuestro ordenamiento jurídico la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las per-

¹ BOE, núm. 44, de 21 de febrero de 2023. Según su Disposición Final Duodécima, su entrada en vigor se produce a los veinte días de su publicación en el BOE.

sonas que informen sobre infracciones del Derecho de la Unión² (en adelante, Directiva 2019/1937 o la Directiva). La nueva norma ya ha provocado diversos comentarios doctrinales³, ante el cúmulo de cuestiones que suscita una mera lectura de su texto. En el presente caso, el objeto de este trabajo se centrará en las implicaciones que la nueva regulación genera en el ámbito penal. Para ello, se abordará la repercusión del nuevo sistema de información en la configuración de la responsabilidad penal de las personas jurídicas⁴ (programas de *compliance*, rol del *compliance officer*, o la eventual afectación del principio *non bis idem* derivada del nuevo régimen sancionador). Seguidamente, se avanzará en una primera aproximación del estudio de algunos de los problemas prácticos que pueden generarse como consecuencia de la puesta en marcha de la ley, particularmente en lo relativo al análisis de determinados elementos estructurales de la investigación de las denuncias internas y su posible efecto en un ulterior proceso penal.

II. EL NUEVO SISTEMA DE INFORMACIÓN Y LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

1. Los programas de *compliance*

Como es conocido, la atribución de la responsabilidad penal a una persona jurídica está basada, en nuestro Derecho, en la realización de una conducta por parte de una persona física, en determinadas circunstancias. Así se expone, literalmente, en el art. 31 bis.1 CP⁵. La jurisprudencia del Tribunal Supremo ha considerado que el fundamento de esta responsabilidad, sobre la que pivota la imputabilidad de la empresa, está basado en la auto responsabilidad motivada por un defecto de organización, como expresión de un obrar corporativo que se coloca al margen del cumplimiento del Derecho. Para la Sala Segunda, no basta con acreditar el delito cometido por la persona física, ya que no existe en esos casos la presunción

² Cuyo texto puede consultarse en <https://www.BOE.es/doue/2019/305/L00017-00056.pdf>.

³ En el apartado de bibliografía se recogen algunos de los que consideramos como de mayor interés.

⁴ Igualmente, en el apartado de bibliografía se contiene una relación de trabajos sobre este tema.

⁵ «[...] las personas jurídicas serán responsables: [...] De los delitos cometidos [...] por [...]».

iuris tantum de que ha concurrido un defecto organizativo. Habrá de probarse que ese delito ha sido una realidad por la concurrencia de un defecto estructural de los mecanismos de supervisión, vigilancia y control exigibles a toda persona jurídica⁶. De forma más matizada, la STS 123/2019, de 8 de marzo (FJ 4) señaló que «la mera inexistencia de formas concretas de vigilancia y control del comportamiento de representantes, directivos y subordinados, tendentes a la evitación de la comisión de delitos imputables a la persona jurídica, no constituye, por sí misma, un comportamiento delictivo. La persona jurídica no es condenada por un (hoy inexistente) delito de omisión de programas de cumplimiento normativo o por la inexistencia de una cultura de respeto al Derecho. [...] Por lo tanto, a la persona jurídica no se le imputa un delito especial integrado por un comportamiento de tipo omisivo, sino el mismo delito que se imputa a la persona física, en el cual, generalmente, participará a través de una omisión de las cauteles obligadas por su posición de garante legalmente establecida, tendentes a evitar la comisión de determinados delitos».

En definitiva, no basta la mera comisión de un delito por una persona física para que, de forma automática, se transfiera la responsabilidad penal a la persona jurídica por cuya cuenta y en su beneficio actúa. De la misma forma, la mera omisión de un programa de *compliance* no supone (ni presupone) la comisión de un delito, de igual modo que su mera existencia tampoco garantiza la impunidad de la estructura societaria⁷. De la doctrina jurisprudencial se deduce que la responsabilidad penal de la persona jurídica está conformada por un presupuesto objetivo, que es la comisión de un hecho delictivo por parte de una persona física, y un presupuesto que pudiéramos considerar como subjetivo, consistente en la deliberada ausencia de un sistema de control (programa de *compliance* o instrumento

⁶ *Vid.*, en tal sentido, desde la controvertida STS 154/2016, de 29 de febrero (FJ 8), pasando por la STS 221/2016, de 16 de marzo (FJ 5.B), que consolidó la posición inicial, que fue reiterada posteriormente en las SSTS 516/2016, de 13 de junio (FJ 1); 583/17, de 19 de julio (FJ 28) y 668/17, de 11 de octubre (FJ 1) hasta llegar a las más recientes SSTS 534/2020, de 22 de octubre (FJ 4) y 470/2021, de 2 de junio (FJ 6). La inequívoca posición del Tribunal Supremo permite prescindir ahora del rico debate sobre si, en realidad, se trata de un sistema de responsabilidad por el hecho propio, basado en una deficiencia organizativa, o de una responsabilidad vicarial. Sobre esta cuestión puede verse mi trabajo: «El sistema vicarial y la carga de la prueba sobre los programas de *compliance* en la responsabilidad penal de las personas jurídicas: hacia la superación de un desencuentro», *Diario La Ley*, núm. 9.221 (2018), sección Documento on-line, 19 de junio.

⁷ *Vid.*, en esta línea, mi trabajo sobre: «La responsabilidad penal de las personas jurídicas: algunas cuestiones sobre el *compliance* y la protección de datos», *La Ley Mercantil*, núm. 55 (2019).

equivalente) que haya posibilitado o no haya impedido de forma razonablemente previsible la comisión de ese hecho delictivo.

La reforma del Código Penal llevada a cabo por la Ley Orgánica 1/2015, de 30 de marzo, introdujo una sustancial modificación de la relevancia de estos programas. Así, antes de la regulación actualmente vigente, los programas de *compliance* venían configurados, esencialmente, como una circunstancia atenuante, cuya relevancia parecía surtir efectos con carácter postdelictual, y respecto de las conductas cometidas por los empleados [art. 31 bis.4.d) CP⁸]. Este régimen se mantiene tras la reforma del año 2015 pero, además, en determinadas circunstancias, estos programas pueden surtir efectos también como eximente, si se implantan con carácter previo a la comisión del delito, y respecto de cualquier persona física cuya actuación determine la atribución de responsabilidad penal a la persona jurídica, es decir, tanto del empleador como del empleado (art. 31 bis, apartados 2, 3, 4 y 5 CP).

La nueva naturaleza de los programas de *compliance*, así como la relevancia que la jurisprudencia ha concedido a este tipo de instrumentos para la propia imputabilidad de la empresa, ha motivado que, en la práctica, el objeto del proceso penal se extienda, de manera esencial, a valorar la idoneidad de estos «modelos de organización y control» —como se les denomina en el art. 31 bis CP—, a fin de determinar la concurrencia o no de una circunstancia eximente de la responsabilidad penal de la entidad. Desde esta perspectiva, resulta palmaria la trascendencia de la nueva norma que ahora se analiza, porque los sistemas de información han de formar parte de un programa de *compliance*, en los términos establecidos en el art. 31 bis.5.4.º CP.

En efecto, el sistema de información contemplado en la nueva ley no debe asimilarse totalmente con un programa de *compliance*, tal y como este viene regulado en el art. 31 bis.5 CP. El sistema, definido en el art. 4 de la Ley 2/2023 como «el cauce preferente para informar sobre las acciones u omisiones» que constituyen su ámbito material de aplicación (art. 2), y que ha de estar conformado por el canal o los canales internos de información (art. 7.1 y 2), puede formar parte, sin duda, del contenido mínimo del programa de *compliance*, que recoge como uno de sus requisitos la «obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención» (art. 31 bis.5.4.º CP). Sin embargo, el programa es mucho más

⁸ En la redacción dada por la Ley Orgánica 5/2010, de 22 de junio.

que un sistema de información. El Código Penal exige un contenido mínimo integrado por los siguientes elementos: un «mapa de riesgos» (art. 31 bis.5-1.º CP); el establecimiento de los procesos de toma de decisiones (art. 31 bis.5-2.º CP); un adecuado sistema de financiación (art. 31 bis.5-3.º CP); un régimen sancionador (art. 31 bis.5-5.º CP); y una actualización periódica (art. 31 bis.5-6.º CP). En todo caso, la trascendencia del cumplimiento de estos requisitos mínimos del programa de *compliance* está ligada a la apreciación como circunstancia eximente de responsabilidad penal para la persona jurídica, pero su real efectividad a tal fin exige, además, su adopción y ejecución eficaz, con carácter previo a la comisión del hecho delictivo, así como su idoneidad para prevenir y perseguir conductas delictivas (art. 31 bis.2 y 4 CP).

Como se puede observar, la nueva norma genera una cierta paradoja. Por un lado, se impone a determinadas entidades (descritas en los arts. 10 y 13 de la Ley 2/2023) el establecimiento de un sistema de información, que es uno de los elementos esenciales de un programa de *compliance*, reforzando así este tipo de herramientas como una pieza clave de la integridad societaria. Pero, por otro, el programa sigue siendo potestativo para las empresas⁹. En cualquier caso, conviene dejar sentado que el sistema de información previsto en la Ley 2/2023 puede ser condición necesaria, pero no suficiente, para que una empresa pueda quedar exenta de responsabilidad penal por los hechos cometidos por sus responsables o empleados. Dicho de otra forma, el cumplimiento de las previsiones legales sobre el sistema de información podría no exonerar, por sí solo, a una empresa de su responsabilidad penal, porque para ello sería necesario cumplir con el resto de las condiciones y requisitos establecidos en el art. 31 bis CP, ya citados. Este peculiar régimen jurídico queda puesto en evidencia en dos aspectos muy concretos. Nos referimos a los responsables del sistema y al régimen sancionador.

⁹ Nos referimos, lógicamente, a la generalidad de las empresas. Cuestión distinta serían aquellas que tienen un régimen peculiar que les exige la implantación de un modelo de cumplimiento normativo. Puede ser útil consultar algunos instrumentos específicos y/o sectoriales existentes en esta materia. Entre otros, se pueden destacar los siguientes: Circulares de la CNMV 6/2009, de 9 de diciembre, «sobre control interno de las sociedades gestoras de instituciones de inversión colectiva y sociedades de inversión», y 1/2014, de 26 de febrero, «sobre los requisitos de organización interna y de las funciones de control de las entidades que presentan servicios de inversión»; Código de Buen Gobierno de las Sociedades Cotizadas, publicado por la CNMV el 24 de febrero de 2015 (revisado en junio de 2020), o los arts. 26 y ss. de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. En otro ámbito, resultan de interés las conocidas como Normas UNE-ISO, entre las que destacan las núms. 37.001, 19.600, 19.601 y 37.301.

2. El rol del *compliance officer*

La Ley del informante establece una clara distinción entre las figuras del «responsable del sistema» de información (art. 8.1) y el «responsable [...] de cumplimiento normativo o de [las] políticas de integridad» (art. 8.6), también conocido como *Compliance Officer*. Se trata, a mi juicio, de una distinción más aparente que real, porque ambas figuras aparecen definidas con un estatus similar dentro de cada entidad. Así, el responsable del sistema es designado por el órgano de administración o de gobierno (art. 8.1 de la Ley 2/2023), como sucede con el *Compliance Officer* (arts. 31 bis.2-1.^a y 2.^a CP)¹⁰. Además, en ambos casos habrán de estar rodeados de las debidas garantías de independencia y autonomía en el ejercicio de sus funciones (art. 8.4 de la Ley 2/2023 y 31 bis.2-2.^a CP), así como contar con los medios personales y materiales suficientes para su desempeño (arts. 8.4 de la Ley 2/2023 y 31 bis.5-3.^o CP).

Sin embargo, la Ley del informante ha querido dejar claro que el responsable del sistema, a su vez, puede ser el responsable del cumplimiento normativo, o no (art. 8.6). Esta cautela puede ser debida, por un lado, al hecho cierto de que no todas las entidades disponen de un programa de *compliance* —y, por tanto, de un *Compliance Officer*— que, insistimos, no es obligatorio para la generalidad de las empresas; o, por otro, a que se haya querido distinguir entre ambas funciones. En este último caso, se hará necesario establecer protocolos muy claros sobre sus respectivas funciones y los sistemas de comunicación entre ambas figuras, para evitar solapamientos competenciales y, sobre todo, para garantizar el correcto funcionamiento del modelo de cumplimiento normativo que, en su caso, se haya implantado en la empresa.

En efecto, como ya se ha expuesto, el sistema de información es solo una parte del programa de *compliance*. Por tanto, las funciones del responsable del sistema y del *Compliance Officer* pueden ser parcialmente coincidentes y, en consecuencia, entrar en colisión. El problema no es tanto la supervisión del sistema de cumplimiento normativo (función propia del *Compliance Officer*, ex art. 31 bis.2-2.^a CP, pero no del responsable del sistema), o recibir denuncias de infracciones (función que, según el art. 31

¹⁰ Incluso, en las denominadas «personas jurídicas de pequeñas dimensiones», el órgano de administración puede asumir las funciones de responsable de cumplimiento (art. 31 bis.3 CP).

bis.5-4.º CP debería ser asumida por el *Compliance Officer* pero que, con la nueva norma, parece residenciarse en el responsable del sistema, como responsable de su «gestión», *ex art. 8.1*, sin perjuicio, en ambos casos, de su delegación)¹¹. La cuestión clave, a mi juicio, es la atribución de la facultad de investigación de esas denuncias.

Sin perjuicio de la posible existencia de un equipo encargado de realizar esta labor, la titularidad o control último de las investigaciones parece atribuirse al responsable del sistema de información, dado que la Ley 2/2023 le confiere expresamente la función de velar por la «tramitación diligente» de las informaciones recibidas (art. 9.1), lo que no parece que pueda referirse exclusivamente a su mera remisión al órgano encargado de hacer la investigación, sino que exigirá, al menos, una función específica de supervisión, coordinación y control de esas tareas de investigación. Sin embargo, la mayor o menor eficacia en esta labor puede tener repercusiones en el ámbito de la responsabilidad penal de la persona jurídica, porque un funcionamiento deficiente del sistema de información puede poner en tela de juicio la eficacia del programa de *compliance*, como requisito determinante de la validez de este como eximente (*ex art. 31 bis.2-1.ª CP*), y cuya responsabilidad corresponde, a su vez, al *Compliance Officer*. De hecho, como ya se expuso, el art. 31 bis.5-4.º CP establece como uno de los requisitos del programa de *compliance* la «obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención», que no es otro que el *Compliance Officer* (*ex art. 31 bis.2-1.ª CP*). No parece tener mucho sentido que la persona encargada de supervisar el funcionamiento del programa de *compliance* y a quien el Código Penal atribuye la función de recibir la información sobre posibles riesgos e incumplimientos no tenga una verdadera facultad de control sobre uno de sus elementos esenciales, como es el sistema interno de información y, con ello, de las propias investigaciones, si con ello puede derivarse la posible exigencia de responsabilidad penal para la empresa. A mi juicio, elementales razones de eficacia y eficiencia aconsejarían que, en aquellas empresas en las que exista la figura del *Compliance Officer*, esta asuma también las funciones de responsable del sistema¹². O,

¹¹ Al margen del ambiguo papel que la Ley 2/2023 otorga al *Compliance Officer*, como perteneciente al «órgano de [...] supervisión de una empresa» y que, al mismo tiempo, puede ser considerado como un informante [*ex art. 3.1.c*].

¹² En mi trabajo sobre «La responsabilidad penal de las personas jurídicas...», *op. cit.*, se defendía la tesis contraria, debido a las altas dosis de formación especializada que se exigen para cumplir cabalmente con las funciones de delegado de protección de datos, lo

en todo caso, que se establecieran con claridad las facultades de supervisión que el responsable del cumplimiento normativo tuviera, a su vez, respecto del responsable del sistema, con la expresa previsión de las situaciones de eventuales conflictos de interés en los casos de denuncias formuladas contra cualquiera de ellos a través del correspondiente canal anónimo, cautela que habrá de extenderse a la designación de la persona encargada de representar a la entidad en un eventual proceso penal (art. 119 LECrim)¹³. Lo que parece claro es que, en las condiciones establecidas por la Ley 2/2023, los órganos de dirección de las empresas afectadas por su ámbito de aplicación habrán de establecer el correspondiente sistema de información (art. 5.1) y designar a su responsable, por lo que una mínima prudencia empresarial aconsejaría la implantación de un modelo integral de cumplimiento normativo, es decir, no solo de un sistema de información sino de un verdadero programa de *compliance*¹⁴.

3. La eventual concurrencia de un *bis in idem*

El art. 63.1.g) de la Ley del informante considera una infracción muy grave el «incumplimiento de la obligación de disponer de un sistema interno de información en los términos exigidos en esta Ley». Si, como hemos visto, la responsabilidad penal de las personas jurídicas está basada en un déficit organizativo por falta de un programa de cumplimiento normativo, rápidamente puede surgir la duda sobre una eventual incursión en el principio proscrito del *bis in idem*. La ausencia de un programa de *compliance* podría constituir, al mismo tiempo, una infracción penal y administrativa.

que aconseja que sea persona distinta al *Compliance Officer*, contribuyendo así a la solidez del modelo de cumplimiento normativo. Por la misma razón, se considera que las figuras del delegado de protección de datos y del responsable del sistema de información deben recaer en personas o entidades diferenciadas. Así parece deducirse también de la propia Ley 2/2023 (arts. 29 y ss.).

¹³ Sobre esta cautela, puede verse la Circular núm. 1/2011 de la FGE que, en su apartado VI.2), instaba a los Fiscales para que cuidaran de que «no se utilice la designación del legal representante de la persona jurídica como un recurso para atribuir indebidamente un estatus similar al del imputado a aquellas personas que deban tener en el proceso una intervención diferente».

¹⁴ Así parece sugerirse también por la Sala Segunda del Tribunal Supremo que, en su STS 316/2018, de 28 de junio, recordada por la STS 470/2021, de 2 de junio, ya distinguía entre el *compliance ad intra* y *ad extra*, es decir, en la conveniencia de contar —en todo tipo de empresas— con este tipo de programas— solo desde la perspectiva de la responsabilidad penal de las personas jurídicas sino como mecanismos de auto protección empresarial frente a conductas de terceros.

Como es conocido, el Tribunal Constitucional ha establecido una doctrina consolidada sobre este principio, que ha sido recientemente reiterada en la STC 2/2023, de 6 de febrero (FJ 4), en la que, con cita de la STC 2/2003, de 16 de enero, y en lo que ahora interesa, se señala lo siguiente:

«c) La garantía del *non bis in idem*, en su vertiente material o sustantiva, prohíbe sancionar dos veces el mismo ilícito si se aprecia identidad de sujetos, hechos y fundamento. [...] Para comprobar si se ha vulnerado el *non bis in idem* cuando se imponen penas y sanciones administrativas, debe atenderse al núcleo esencial de esta garantía: impedir el exceso de punición. Por ello, “no cabe apreciar una reiteración punitiva constitucionalmente proscrita cuando, aun partiéndose de la existencia de la imposición de una doble sanción en supuestos de identidad de sujeto, hecho y fundamento, en la ulterior resolución sancionadora se procede a descontar y evitar todos los efectos negativos anudados a la previa resolución sancionadora, ya que, desde la estricta dimensión material, [el descuento] provoca que en el caso concreto no concurra una sanción desproporcionada (STC 334/2005, de 20 de diciembre, FJ 2)”. [...]

d) La garantía del *non bis in idem*, en su vertiente procesal o procedimental, ubicada en el ámbito del derecho a la tutela judicial efectiva (art. 24.1 CE), conlleva, ante todo, según nuestra doctrina, la interdicción de un doble proceso penal con el mismo objeto [...].

El art. 14.7 del Pacto internacional de derechos civiles y políticos y el art. 4 del Protocolo 7 al Convenio europeo de derechos humanos “protegen al ciudadano no solo frente a la ulterior sanción —administrativa o penal—, sino frente a la nueva persecución punitiva por los mismos hechos una vez que ha recaído resolución firme en el primer procedimiento sancionador, con independencia del resultado —absolución o sanción— del mismo”. Sin embargo, la prohibición constitucional del doble enjuiciamiento fuera del proceso penal solo procederá en aquellos casos en que el procedimiento administrativo sancionador le sea equiparable, “en atención a las características del procedimiento —su grado de complejidad— como a las de la sanción que sea posible imponer en él —su naturaleza y magnitud— [...]” [...].

La doctrina del Tribunal Europeo de Derechos Humanos mantiene una posición semejante en la STEDH, Gran Sala, de 15 de noviembre de 2016, asunto *A y B c. Noruega* [...] [que] considera legítima una respuesta sancionadora penal y administrativa complementaria frente a ciertos comportamientos socialmente inaceptables (por ejemplo, el incumplimiento de las leyes de tráfico, el impago de impuestos o la evasión fiscal) [...] siempre que estos procedimientos se combinen de manera integrada y formen un todo coherente, lo que implica, por un lado, que los fines perseguidos

y los medios utilizados para alcanzarlos sean, en esencia, complementarios y estén vinculados en el tiempo (lo que denomina “existencia de un vínculo material y temporal suficientemente estrecho”) y, por otro, que las consecuencias de organizar así la respuesta sancionadora frente a aquella clase de infracciones sean previsibles y proporcionadas para la persona afectada (§§ 121, 123 y 130) [...].

Entre los criterios citados por la sentencia A y B c. Noruega para decidir si existe un vínculo material suficientemente estrecho destaca, sobre todo, el de si la sanción impuesta en el procedimiento que finaliza en primer lugar se tiene en cuenta en el que finaliza en el último, para evitar que la persona afectada acabe soportando una carga excesiva, riesgo este último menos probable cuando existe un mecanismo de compensación que garantice que el *quantum* global de las sanciones impuestas sea proporcionado (§ 132)»¹⁵.

Sentado lo anterior, un análisis estricto de la cuestión permitiría avalar, aunque con ciertas cautelas, la tesis de la inexistencia de un *bis in idem*.

En primer lugar, es preciso recordar, como ya se expuso anteriormente, que el sistema de información no puede ser equiparado con el programa de *compliance*, sino, en su caso, con uno de los requisitos esenciales para que este pueda operar como eximente de la responsabilidad penal de la persona jurídica (ex art. 31 bis.5-4.º CP). Por tanto, la ausencia de un sistema de información no puede ser asimilada, sin más, con la falta de un programa de *compliance*, que es un instrumento mucho más amplio, por lo que podría entenderse que no concurre el requisito de la identidad del hecho determinante de la prohibición del *bis in idem*.

En segundo lugar, desde la perspectiva del fundamento de la sanción también podrían encontrarse diferencias sustanciales ya que, aunque es cierto que tanto la regulación de la responsabilidad penal de las personas jurídicas como la Ley del informante son herramientas de promoción de la cultura del cumplimiento normativo de las empresas, no puede ocultarse que la Ley 2/2023 responde, como se recoge en su art. 1, a una concreta finalidad que es la protección de los denunciantes de infracciones. De esta

¹⁵ De forma esencialmente compatible con esta doctrina del TEDH, asumida por el TC, se pronuncia el TJUE (GS) en su Sentencia de 20 de marzo de 2018 (asunto *Menci*), citada en la STS 320/2022, de 30 de marzo, y en la que se hace referencia a los denominados «criterios Engel» (STEDH de 8 de junio de 1976), sobre la equiparación de las sanciones administrativas y penales, teniendo en cuenta su definición o calificación jurídica en el derecho del estado correspondiente, la naturaleza de la infracción y el grado de severidad de la sanción que puede sufrir el interesado (parágrafo 82).

forma, la sanción administrativa encuentra su fundamento en la necesidad de establecer un mecanismo seguro de comunicación de infracciones y de garantía de indemnidad del denunciante, mientras que el régimen jurídico previsto en los arts. 31 bis y ss. CP entronca con los principios de prevención general y especial propios del Derecho penal, puestos en relación con cada uno de los tipos delictivos que admiten esta figura, es decir, ofrece una respuesta punitiva ante un bien jurídico mucho más amplio que la mera protección de un denunciante.

Sin embargo, no es posible descartar algún caso hipotético en que el programa de *compliance* no haya podido surtir efecto como eximente para la empresa, precisamente por no contener un sistema interno de información. En tales casos, podría plantearse no solo una eventual coincidencia de hecho y de sujeto, sino una posible compatibilidad de las vías penal y administrativa, atendiendo a la complementariedad de la respuesta del estado frente a ciertos comportamientos socialmente inaceptables (en los términos expuestos por el TEDH). En este tipo de supuestos, la solución concreta no parece sencilla, porque habrá que atender a la conexión material y temporal de ambos procedimientos, así como a la naturaleza y gravedad de las sanciones, que pueden resultar sustancialmente coincidentes o no en el caso de las de carácter pecuniario, cuya previsibilidad puede resultar inicialmente indeterminada en función de los propios criterios establecidos en los arts. 33.7 CP y 65.1.b) de la Ley 2/2023¹⁶. En cualquier caso, siempre quedará la posibilidad de aplicar la correspondiente compensación en el segundo procedimiento, de manera que, materialmente, solo se imponga una sanción, la primera, a fin de evitar el «exceso de punición» como núcleo esencial de la garantía del *bis in idem*.

III. EL NUEVO SISTEMA DE INFORMACIÓN Y SU POSIBLE EFECTO EN EL PROCESO PENAL

Si las cuestiones abordadas en los apartados anteriores pueden presentarse problemáticas, otro tanto sucede con la aplicación práctica del sistema de información, una vez se recibe la denuncia correspondiente, porque el procedimiento que se siga para la verificación y, en su caso, sanción de

¹⁶ El art. 33.7.a) CP prevé pena de multa «por cuotas o proporcional», a determinar en cada tipo delictivo; mientras que el art. 65.1.b) de la Ley 2/2023 sanciona las infracciones muy graves con multas de entre 600.001 y 1.000.000 de euros, a modular conforme a los criterios previstos en el art. 66.

las infracciones cometidas, puede tener una seria repercusión en un eventual procedimiento penal posterior, frente a personas físicas o jurídicas. En este punto, solo pretendemos hacer una primera aproximación, en el convencimiento de que el desarrollo práctico de la norma suscitará muchos más interrogantes.

Ante todo, conviene señalar que, como ya se ha avanzado, la finalidad de la Ley 2/2023 aparece descrita en su art. 1, y consiste en «otorgar una protección adecuada frente a las represalias que puedan sufrir» los informantes y, al mismo tiempo, fortalecer la «cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público». En suma, la Ley no está pensada para la investigación de hechos delictivos, sino para la protección de los eventuales denunciadores y el fomento de los canales de información o comunicación de infracciones. Estos objetivos solo pueden entenderse como una de las vertientes de la cuestión de fondo que debería merecer especial atención, y sobre la que poco se dice en el texto de la norma, que es el impulso de la cultura del cumplimiento normativo¹⁷, como mecanismo eficaz de prevención de conductas delictivas cometidas en el seno de las empresas. Quizá lastrada por la finalidad estricta de la Directiva¹⁸, creo que se ha perdido una buena oportunidad para reforzar esa idea central que, a mi juicio, debería presidir este tipo de normas, dentro de un objetivo general más amplio en el que se contemplara un verdadero plan estratégico de lucha contra la corrupción, que solo aparece tímidamente apuntado en la disposición adicional quinta¹⁹.

En cualquier caso, este alcance limitado de la norma puede explicar el sorprendente silencio normativo sobre el contenido de la investigación a realizar en el marco del sistema de información diseñado por la Ley 2/2023²⁰.

¹⁷ Que ahora parece denominarse «infraestructuras de integridad de las organizaciones».

¹⁸ Su objetivo declarado en el art. 1 también es proporcionar «un elevado nivel de protección de las personas que informen sobre infracciones del Derecho de la Unión».

¹⁹ «El Gobierno, en el plazo máximo de dieciocho meses a contar desde la entrada en vigor de la presente ley, y en colaboración con las Comunidades Autónomas, deberá aprobar una Estrategia contra la corrupción que al menos deberá incluir una evaluación del cumplimiento de los objetivos establecidos en la presente ley así como las medidas que se consideren necesarias para paliar las deficiencias que se hayan encontrado en ese periodo de tiempo».

²⁰ Los posibles efectos perniciosos del clamoroso silencio legal ya han sido advertidos por el presidente de la Sala Segunda del Tribunal Supremo. Puede verse en el siguiente enlace: <https://confilegal.com/20230310-marchena-desconfia-del-investigador-interno-de-empresa-contemplado-en-la-nueva-ley-de-alertadores-de-corrupcion/>.

El art. 19.1 simplemente establece que la «instrucción [término con una clara connotación penal] comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados», pero este precepto solo contempla las investigaciones realizadas por la Autoridad Independiente de Protección del Informante, AAI, no por las propias empresas.

Por su parte, el art. 39 señala que las personas afectadas por el expediente «tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley». Sin embargo, en el caso concreto de las investigaciones llevadas a cabo por la Autoridad Independiente de Protección del Informante, AAI, estos derechos pueden resultar notablemente restringidos. El art. 19.2 permite que la persona investigada tenga noticia de la información o comunicación y de los hechos denunciados, así como del derecho a presentar alegaciones por escrito, en el trámite de audiencia, no antes, si «se considerara que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas», consagrando de esta forma una especie de «secreto de las actuaciones» *de facto*, cuyo presupuesto de hecho queda al ponderado criterio del instructor del expediente...

Tan escuetas referencias permiten atisbar algunos nubarrones en la puesta en práctica de la Ley, cuando se trate de verificar la existencia de hechos que pudieran revestir caracteres delictivos. La obligación de remisión «inmediata» al Ministerio Fiscal [art. 9.2.j)], no impide que, al menos en abstracto, puedan darse casos en que sea necesario depurar los hechos denunciados, antes de su calificación jurídica como delito. Esa depuración no es propiamente una investigación penal, pero podrían practicarse diligencias que deriven en la verificación de un hecho delictivo. Surgen entonces las dudas sobre el régimen de derechos y garantías que hayan de revestir esas diligencias y su eventual efecto en un ulterior proceso penal. Con la finalidad de contribuir a los debates que, sin duda, se plantearán, y con el ánimo de ofrecer algunas soluciones a los problemas que se puedan suscitar, se abordarán a continuación algunas de las cuestiones que me parecen más relevantes.

1. El concepto de denunciante y su necesaria contextualización

Como se ha expuesto, una de las finalidades esenciales de la norma es dotar de una adecuada protección a toda aquella persona que denuncie

alguna de las infracciones previstas en su ámbito material de aplicación (art. 2 de la Ley 2/2023²¹). Lógicamente, solo puede protegerse al denunciante que se identifica como tal. Sin embargo, la norma admite también la denuncia anónima (arts. 7.3 y 17.1), en coherencia con lo dispuesto en el art. 6.2 de la Directiva. De hecho, el art. 35.2 de la Ley 2/2023 garantiza la protección a quienes, habiendo denunciado de forma anónima, hayan sido identificados con posterioridad.

El denunciante anónimo es quien formula la denuncia sin ofrecer dato alguno que permita su identificación (STS 318/2013, de 11 de abril de 2013, FJ 2). Respecto de este tipo de denuncias, existe una consolidada doctrina del Tribunal Supremo que, en el ámbito penal, advierte de que debe ser «objeto de un juicio de ponderación reforzado», sin perjuicio de admitir su viabilidad como instrumento para la puesta en conocimiento de un hecho delictivo que justifique la apertura de una investigación, una vez que «su destinatario valore su verosimilitud, credibilidad y suficiencia» (STS 141/2020, de 13 de mayo, FJ 2.3)²². Nada impide que esta cautela

²¹ «a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que: 1.º Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno; 2.º Afecten a los intereses financieros de la Unión Europea tal y como se contemplen en el art. 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o 3.º Incidan en el mercado interior, tal y como se contempla en el art. 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades. b) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social». La propia Ley excluye de su ámbito de protección las denuncias que afecten a la información clasificada, al secreto profesional de los profesionales de la medicina y la abogacía, al deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad, y al secreto de las deliberaciones judiciales (art. 2.4), así como a las informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado (art. 2.5).

²² En la reciente Circular 2/2022, de 20 de diciembre, sobre la actividad extraprocesal del Ministerio Fiscal en el ámbito de la investigación penal (apartado 4.2.3), la Fiscalía General del Estado no solo reitera las consideraciones ya expuestas en la Instrucción 3/1993, sino que parece decantarse abiertamente a favor de este tipo de denuncias.

deba ser igualmente observada en el marco de la aplicación de la norma ahora analizada, sobre todo si los hechos comunicados pudieran revestir los caracteres propios de una infracción penal.

La figura del denunciante anónimo debe ser distinguida de la preservación de la identidad del informante, garantía que aparece recogida en el art. 19.2 de la Ley 2/2023 como excepción a los derechos reconocidos a la persona investigada, y que figura ligada a la protección de datos personales en el art. 33.1 de la Ley 2/2023. Esta garantía asegura la no difusión al denunciado ni a terceros de los datos de identificación del denunciante obrantes en el expediente. No obstante, conviene aclarar que esta garantía decae cuando se trata de la actuación de una Autoridad judicial, del Ministerio Fiscal o de la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora (art. 33.3), a quienes se podrá comunicar la identidad del denunciante, previa comunicación a este²³.

En cualquier caso, para que un informante pueda acogerse a las medidas de protección establecidas en los arts. 35 y ss. de la norma, es necesario

Así, se afirma lo siguiente: «Actualmente, nos encontramos inmersos en una sociedad digital fuertemente interconectada en la que toda la ciudadanía resulta potencial receptora y difusora de información. En opinión de la doctrina, es de prever que las delaciones anónimas se vean notablemente incrementadas fruto de la consolidación de una corriente social caracterizada por un singular compromiso en la ejecución de tareas de auxilio y colaboración con la Administración de Justicia y, desde luego, como consecuencia del cada vez más extendido uso de las nuevas tecnologías como vehículo de transmisión de la noticia criminal. Frente a los tradicionales recelos suscitados por la delación anónima, hoy en día se reputa una medida útil para potenciar la colaboración con la justicia. Diversos instrumentos legales incentivan y promueven la creación de buzones de colaboración ciudadana y canales de denuncia interna que garanticen el anonimato o, cuando menos, la confidencialidad del denunciante. La Guía Técnica de la Convención de Naciones Unidas contra la Corrupción, aprobada en 2010, señala que “convendría, tal vez, que los Estados parte consideraran la viabilidad de garantizar el anonimato de los denunciantes”, sugerencia que, a su vez, se reitera en el Programa anticorrupción de ética y cumplimiento para las empresas, elaborado por Naciones Unidas en el año 2013. En el ámbito europeo constituyen un claro exponente de esta nueva tendencia tanto la Directiva UE 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, como la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informan sobre infracciones del derecho de la Unión».

²³ La norma no dice nada sobre las consecuencias de una eventual negativa del denunciante, que debe entenderse irrelevante a estos efectos. Como tampoco resulta clara la necesidad de informar previamente a todo denunciante de esta posibilidad. De cualquier manera, en el ámbito penal, podría seguir siendo de aplicación lo dispuesto en la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, siempre que concurran los requisitos establecidos en esta norma.

que la comunicación se haya realizado conforme a los requerimientos previstos en la Ley. Y, en este punto, la norma excluye de su ámbito de protección —entre otras— aquellas informaciones «que ya estén completamente disponibles para el público» (art. 35.2.c)]. En esta materia concreta contamos con una reciente STEDH (GS) de 14 de febrero de 2023 (asunto *Halet c. Luxemburgo*) que ofrece algunas pautas para definir el concepto propio de denunciante a los efectos de obtener la adecuada protección, y de la que se puede derivar su naturaleza «relacional» o «contextualizada».

El supuesto de hecho consistía en la entrega a un periodista de varias declaraciones fiscales de empresas para su utilización en un programa de televisión, a raíz de la previa revelación por otro empleado de la misma empresa de varios centenares de documentos fiscales confidenciales, remitidos a medios de comunicación con la finalidad de llamar la atención sobre los acuerdos fiscales ventajosos celebrados entre algunas multinacionales y las autoridades de Luxemburgo. La Gran Sala, en contra del criterio de la primera instancia, consideró que se había vulnerado el derecho del demandante reconocido en el art. 10 CEDH, atendiendo a que la naturaleza, gravedad y efecto disuasorio de la sanción penal impuesta suponían una injerencia innecesaria en una sociedad democrática para su derecho a la libertad de expresión, en particular, para la libertad de difundir información de interés público (§ 206).

Ante la falta de una definición jurídica uniforme a nivel internacional y europeo, el TEDH no ofreció un concepto abstracto y general de *whistle-blower* (denunciante), pero sí apuntaló los tres criterios relevantes para la aplicación del régimen de protección correspondiente (§§ 116-119): *i*) si el empleado o funcionario en cuestión era la única persona, o parte de una pequeña categoría de personas, consciente de lo que estaba ocurriendo en el trabajo; *ii*) el deber de lealtad, reserva y discreción inherente a una relación laboral y, en su caso, la obligación de cumplir un deber legal de secreto, y *iii*) la posición de vulnerabilidad económica frente a la persona, institución pública o empresa de la que dependían para su empleo y el riesgo de sufrir represalias. A tal efecto, el Tribunal realizó un ejercicio de ponderación que, en lo esencial, se expondrá a continuación.

En primer lugar, los canales utilizados para hacer la revelación (§§ 121-123). En principio, la denuncia debe hacerse a través del canal interno, pero determinadas circunstancias pueden justificar el uso directo de una denuncia ante terceros, incluidos los medios de comunicación. En concreto, cuando el canal interno no sea fiable o se haya revelado como ineficaz, o cuando exista una probabilidad de represalias. En ese caso, no estaba

en cuestión la autenticidad de la información (§§ 124-127) ni la buena fe (§§ 128-130) del demandante.

En segundo lugar, el interés público de la información divulgada (§§ 131-144), que debe valorarse junto con los intereses que el deber de secreto pretende proteger (sobre todo, cuando la revelación afecta a terceras empresas, como era el caso). En esta línea, el Tribunal considera que el interés público de la información divulgada puede ir disminuyendo gradualmente en función de si la información se refiere a actos o prácticas ilícitas; a actos, prácticas o conductas reprobables; o a un asunto que suscita un debate que da lugar a una controversia sobre la existencia o no de un perjuicio para el interés público. En este caso, en el que se habían producido revelaciones previas, el Tribunal aclaró que el mero hecho de que ya se hubiera iniciado un debate público cuando se produjo la difusión no podía, *per se*, excluir la posibilidad de que la información revelada también hubiera sido de interés público. Más en concreto, el TEDH entendió que los documentos difundidos habían contribuido a la transparencia de las prácticas fiscales de las empresas multinacionales que tratan de trasladar sus beneficios a países de baja tributación, así como sobre las opciones políticas adoptadas por Luxemburgo en este ámbito. Por tanto, la divulgación había sido de interés público, no solo para este país, sino también para Europa y los demás Estados cuyos ingresos fiscales podían verse afectados por dichas prácticas.

En tercer lugar, el perjuicio causado (§§ 145-148), en el que debía valorarse no solo el de la empresa para la que trabajaba el demandante, sino también otros intereses privados de terceros, así como los intereses públicos (por ejemplo, el bien económico general, la confianza de los ciudadanos en la equidad y justicia de las políticas fiscales de los Estados, la prevención y/o sanción de conductas como la sustracción o difusión indebida de datos, o la necesidad de preservar el secreto profesional). Tras realizar el correspondiente ejercicio de ponderación, el Tribunal concluyó que el interés público de la divulgación impugnada prevalecía sobre todos los efectos perjudiciales.

En cuarto lugar, la gravedad de la sanción impuesta al demandante (§§ 149-154). El Tribunal considera que, en función del contenido de la revelación y de la naturaleza del deber de confidencialidad o de secreto violado por esta, el comportamiento del interesado podía legítimamente constituir una infracción penal. Por otra parte, ni el art. 10 CEDH ni la jurisprudencia del Tribunal excluyen la posibilidad de que un mismo acto pueda dar lugar a un conjunto de sanciones o dar lugar a múltiples repercusiones,

ya sean profesionales, disciplinarias, civiles o penales. No obstante, en el caso concreto, y teniendo en cuenta la naturaleza de las sanciones impuestas y la gravedad de su efecto acumulativo y, en particular, su efecto desalentador para el ejercicio del derecho invocado, el Tribunal consideró que la condena penal del demandante había sido desproporcionada.

2. Los derechos y obligaciones de las partes implicadas y su eventual repercusión para la persona jurídica

En nuestro Derecho no existe una genérica obligación legal de denunciar, entendida como una conducta que, de no llevarse a cabo, derive en una responsabilidad penal²⁴. Partiendo de esa base, las informaciones contempladas en la Ley 2/2023 obedecerán —en condiciones normales— a una decisión libre y voluntaria del denunciante. El establecimiento de un sistema interno o externo de información puede facilitar o fomentar las denuncias, pero no las convierte en obligatorias, es decir, no altera el esquema normativo general ya expuesto.

Por otro lado, el art. 24.2 CE garantiza los derechos a no declarar contra sí mismo y a no confesarse culpable. Como se expuso en la STC 181/2020, de 14 de diciembre (FJ 2), estos derechos han de ser contemplados «no solo desde la perspectiva de su relevancia para los derechos de la persona detenida, como garantía de protección de su derecho a la libertad frente a la actuación gubernativa, sino también por la indudable proyección en el eventual proceso penal que, en su caso, sea incoado»; derechos que, a su vez, están «estrechamente relacionados con los de defensa y a la presunción de inocencia, de los que constituyen una manifestación concreta». El reconocimiento de estos derechos se sustenta en la consideración del denunciado como «sujeto» del proceso, no como su «objeto», a quien debe «reconocérsele la necesaria libertad [...] para defenderse [...] en la forma que estime más conveniente para sus intereses». De manera que el contenido esencial de tales derechos es «la interdicción de la compulsión del testimonio con-

²⁴ Las únicas excepciones vienen expresamente recogidas en el art. 408 CP, que sanciona a la «autoridad o funcionario que, faltando a la obligación de su cargo, dejare intencionadamente de promover la persecución de los delitos de que tenga noticia o de sus responsables»; y en el art. 450 CP, que castiga a quien «pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual» o a quien «pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan un delito de los previstos en el apartado anterior y de cuya próxima o actual comisión tenga noticia».

tra uno mismo (STC 161/1997, de 2 de octubre, FJ 6) y el reconocimiento de la necesaria libertad para declarar o no y para hacerlo en el sentido que se estime más conveniente (STC 142/2009, de 15 de junio, FJ 3)», sin que pueda derivarse consecuencia negativa alguna de su actitud²⁵.

Sin embargo, en el caso de que nos encontremos ante una conducta delictiva cometida en el seno de una persona jurídica, resulta necesario plantearse hasta qué punto la denuncia formulada por un empleado de la empresa o su reconocimiento de los hechos puede implicar una eventual vulneración del derecho de la propia empresa a no declarar contra sí misma y a no confesarse culpable. En principio, podemos señalar que la heterorresponsabilidad atribuida a la persona jurídica, como elemento de alteridad, permite descartar cualquier vulneración en un supuesto como ese.

En efecto, como ya se expuso, la doctrina jurisprudencial actual considera que la atribución de responsabilidad penal a la persona jurídica requiere un presupuesto objetivo, que es la comisión de un hecho delictivo por parte de una persona física, y un presupuesto que pudiéramos considerar como subjetivo, consistente en la deliberada ausencia de un sistema de control (programa de *compliance* o instrumento equivalente) que haya posibilitado o no haya impedido de forma razonablemente previsible la comisión de ese hecho delictivo. De tal manera que la comisión de un hecho delictivo por una persona física no implica que se transfiera su responsabilidad penal, sin más, a la persona jurídica. Es necesario que esta, a su vez, haya incurrido en un «defecto organizativo» o en un «defecto estructural en los modelos de gestión, vigilancia y supervisión»²⁶. Por tanto, la mera denuncia o reconocimiento de un particular, haya sido o no el autor material del hecho punible, en la que se ponga de manifiesto la comisión de un hecho delictivo en el seno de una persona jurídica, no puede implicar el reconocimiento de la responsabilidad penal de esta, puesto que esa responsabilidad no deriva directamente de la conducta del particular, sino de su propia conducta, que podrá concurrir o no, y sobre la que podrá ejercer su derecho de defensa. A tal efecto, la única persona que, en puridad, puede vincular a la persona jurídica en su posición pro-

²⁵ No obstante, el Tribunal Constitucional ha aceptado, «mediante expresa invocación de la doctrina sentada en el caso *Murray* del Tribunal Europeo de Derechos Humanos [que pueda] justificarse que se extraigan consecuencias negativas del silencio cuando, existiendo pruebas incriminatorias objetivas al respecto, cabe esperar del imputado una explicación (STC 202/2000, de 24 de julio, FJ 3)» (STC 9/2011, de 28 de febrero (FJ 5).

²⁶ En palabras de la STS 221/2016, de 16 de marzo (FJ 5.B).

cesal, declarando contra sí misma o admitiendo su culpabilidad, es la figura del «representante» prevista en el art. 119.1.a) LECrim, es decir, de la persona física designada por la entidad para que actúe en su nombre en el procedimiento. Como expone el art. 786 bis LECrim, esa persona «podrá declarar en nombre de la persona jurídica si se hubiera propuesto y admitido esa prueba, sin perjuicio del derecho a guardar silencio, a no declarar contra sí mismo y a no confesarse culpable, así como ejercer el derecho a la última palabra al finalizar el acto del juicio». Añadiendo el art. 787.8 LECrim que la conformidad «deberá prestarla [este] representante especialmente designado, siempre que cuente con poder especial».

No obstante lo anterior, conviene señalar que, tal y como se recoge en la Circular núm. 1/2016, de 22 de enero, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015 (apartado 5.6), uno de los criterios relevantes para valorar la idoneidad de un programa de *compliance* es su capacidad para detectar las conductas delictivas. De manera que si el hecho delictivo ha sido advertido y denunciado por la propia entidad (por ejemplo, a través del *Compliance Officer*, por sí mismo o previa denuncia de algún integrante de la empresa) podrá apreciarse como elemento indicativo de la eficacia del modelo y su correspondencia con una cultura de compromiso corporativo, a los efectos de su eventual ponderación como circunstancia atenuante o eximente.

3. El contenido de la investigación: algunos supuestos problemáticos

Una vez recibida la comunicación a través del canal interno de información, la Ley 2/2023 no regula el contenido de la investigación que, en su caso, pueda desarrollarse en el seno de la entidad para alcanzar alguna conclusión sobre la verosimilitud de lo denunciado, la o las personas responsables, y las eventuales consecuencias o medidas a adoptar. Surgen entonces las lógicas dudas sobre el alcance de la actuación que puede llevarse a cabo por quien haya sido designado como «instructor» o responsable de la tramitación de esa información. Como luego veremos, no debería existir mayor dificultad en tomar declaración al propio denunciante, si está identificado, o a los posibles testigos, así como recibir y analizar la documentación aportada, en su caso. Se trata, en todo caso, de diligencias que podrían —y deberían— ser reiteradas en el eventual proceso penal que pudiera ser incoado con posterioridad, sin tacha de nuli-

dad alguna derivada de su práctica en el ámbito de la investigación interna. Más problemas plantea la utilización de determinados instrumentos de investigación —o de su resultado—, que pudieran afectar a los derechos fundamentales de los implicados, a fin de garantizar su futura validez probatoria en el marco del proceso penal. En este punto, por su interés y utilidad práctica, nos permitimos recordar la doctrina del Tribunal Europeo de Derechos Humanos, del Tribunal Constitucional y del Tribunal Supremo sobre dos medidas de investigación: el análisis de los dispositivos electrónicos puestos a disposición de los trabajadores y las grabaciones obtenidas a través de los sistemas de videovigilancia instalados en las empresas por motivos de seguridad.

3.1. *El análisis de los dispositivos electrónicos puestos a disposición de los trabajadores (la doctrina Barbulescu)*

La STEDH de 5 de septiembre de 2017 (asunto *Barbulescu c. Rumanía*) abordó el enjuiciamiento de una eventual vulneración del art. 8 CEDH (derecho a la «vida privada»), derivada de la monitorización por el empresario de las comunicaciones mantenidas por el trabajador a través de la aplicación informática de mensajería denominada *Yahoo Messenger*, y su uso con fines disciplinarios en el ámbito laboral.

El TEDH reconoce que la «noción de “vida privada” puede incluir las actividades profesionales» (§ 71); que el demandante «había sido efectivamente informado de la prohibición de utilizar personalmente internet», pero «no está tan claro que se le hubiera informado antes del seguimiento de sus comunicaciones de que se iba a realizar esa operación de monitorización» (§ 77); que, «en todo caso, no parece que el demandante haya sido informado con antelación del alcance y la naturaleza de las actividades de monitorización de su empresario, ni de la posibilidad de que este tenga acceso al contenido real de sus comunicaciones» (§ 78), y que, en cualquier caso, «las instrucciones de un empresario no pueden reducir a cero la vida social privada en el lugar de trabajo» (§ 80). Concluye señalando que «las comunicaciones del demandante en el lugar de trabajo estaban comprendidas en los conceptos de “vida privada” y “correspondencia”» (§ 81).

El TEDH considera que el derecho laboral «tiene características específicas que deben tenerse en cuenta. La relación empresario-empleado es contractual, con derechos y obligaciones particulares para ambas partes, y se caracteriza por la subordinación jurídica» (§ 117). «Desde una perspec-

tiva regulatoria, el derecho laboral deja un margen de negociación entre las partes en el contrato de trabajo» (§ 118). El «Tribunal considera que debe concederse a los Estados contratantes un amplio margen de apreciación al evaluar la necesidad de establecer un marco jurídico que regule las condiciones en que un empresario puede regular las comunicaciones electrónicas o de otro tipo de carácter no profesional de sus empleados en el lugar de trabajo» (§ 119). «No obstante, la discreción [discrecionalidad] de que gozan los Estados en este ámbito no puede ser ilimitada» (§ 120). Por ello se establecen unos criterios generales que habrán de ser ponderados por los Estados (§ 121):

«i) Si se ha notificado al empleado la posibilidad de que el empresario adopte medidas para supervisar la correspondencia y otras comunicaciones, y la implementación de esas medidas. Si bien en la práctica los empleados pueden ser notificados de diversas maneras en función de las circunstancias fácticas particulares de cada caso, el Tribunal considera que para que las medidas se consideren compatibles con los requisitos del art. 8 del Convenio, la notificación debería normalmente ser clara sobre la naturaleza de la supervisión y darse con antelación;

ii) El alcance de la supervisión por parte del empresario y el grado de intrusión en la intimidad del empleado. A este respecto, debe distinguirse entre la monitorización del flujo de comunicaciones y de su contenido. También debe tenerse en cuenta si se han monitorizado todas las comunicaciones o solo parte de ellas, así como la cuestión de si la monitorización fue limitada en el tiempo y el número de personas que tuvieron acceso a los resultados [...]. Lo mismo se aplica a los límites espaciales de la monitorización;

iii) Si el empresario ha proporcionado razones legítimas para justificar la monitorización de las comunicaciones y el acceso a su contenido real [...]. Dado que la monitorización del contenido de las comunicaciones es, por naturaleza, un método claramente más invasivo, requiere una justificación más ponderada;

iv) Si hubiera sido posible establecer un sistema de supervisión basado en métodos y medidas menos intrusivos, que el acceso directo al contenido de las comunicaciones del empleado. A este respecto, debería evaluarse, a la luz de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario podría haberse logrado sin haber accedido directamente al contenido completo de las comunicaciones del empleado;

v) Las consecuencias del control para el empleado sometido a él [...]; y la utilización por el empresario de los resultados de la operación de monitorización, en particular si los resultados se utilizaron para alcanzar el objetivo declarado de la medida [...];

vi) Si se habían proporcionado al empleado las garantías adecuadas, especialmente cuando las operaciones de supervisión del empresario eran de carácter intrusivo. Esas garantías deben garantizar, en particular, que el empresario no pueda acceder al contenido real de las comunicaciones en cuestión a menos que el empleado haya sido notificado con antelación de esa eventualidad».

En definitiva, el TEDH reconoce que el derecho a la «vida privada» (art. 8.1 CEDH), cuya traslación en nuestro derecho puede reconducirse al derecho a la intimidad personal (art. 18.1 CE), con ciertos matices —STC 66/2022, de 2 de junio [FJ 4.A.c)]—, presenta características específicas en el ámbito laboral. Y, a pesar de admitir un amplio margen de regulación a las legislaciones nacionales, establece una serie de criterios a tener en cuenta a esos efectos. Criterios que, conocidos como «test *Barbulescu*», se han convertido en parámetros ponderativos que han de ser valorados por los tribunales en la resolución de los asuntos que se les sometan a su consideración.

De esta forma, en el caso concreto, el TEDH concluye que «los tribunales nacionales no determinaron, en particular, si el demandante había recibido una notificación previa de su empresa sobre la posibilidad de monitorizar sus comunicaciones en *Yahoo Messenger*; tampoco tuvieron en cuenta el hecho de que no había sido informado de la naturaleza o el alcance de la supervisión, ni el grado de intrusión en su vida privada y su correspondencia. Además, no determinaron, en primer lugar, las razones concretas que justificaban la introducción de las medidas de monitorización; en segundo lugar, si el empresario podría haber utilizado medidas que implicaran una menor intrusión en la vida privada y la correspondencia del demandante; y en tercer lugar, si se podría haber accedido a las comunicaciones sin su conocimiento (*vid.* párrafos 120 y 121 *supra*)» (§ 140). Por ello, «y a pesar del margen de apreciación del Estado demandado, el Tribunal considera que las autoridades nacionales no protegieron adecuadamente el derecho del demandante al respeto de su vida privada y su correspondencia y que, por consiguiente, no lograron una ponderación justa entre los intereses implicados. Por lo tanto, se ha producido una violación del art. 8 del Convenio» (§ 141).

La doctrina *Barbulescu* ha sido asumida por la Sala Cuarta (de lo Social) del Tribunal Supremo en las SSTS 119/2018, de 8 de febrero (FJ 7) y 221/2022, de 14 de marzo (FJ 4), entre otras; y por el Tribunal Constitucional en la STC 160/2021, de 4 de octubre [FJ 3.b)].

En el ámbito penal, resulta especialmente relevante la STS 489/2018, de 23 de octubre, en la que se asume la doctrina *Barbulescu*.

En esta sentencia se abordaba un supuesto de informe pericial basado en la realización de una «copia espejo» del contenido del ordenador laboral de un empleado que había sido despedido el día anterior, ante la existencia de vehementes sospechas de conductas desleales (participación en otras empresas dedicadas a la misma actividad que su principal). La resolución, con una evidente vocación pedagógica, expone con brillantez la doctrina constitucional sobre el derecho a la intimidad (art. 18.1 CE), y sus diferencias con los derechos al secreto de las comunicaciones (art. 18.3 CE) y a la protección de datos personales y al entorno digital (art. 18.4 CE). Así, no es lo mismo intervenir en un proceso de comunicación en marcha que en un proceso de comunicación cerrado. Tampoco es lo mismo indagar sobre una concreta comunicación que proceder al registro de un dispositivo de almacenamiento masivo de información (actualmente regulado en los arts. 588 sexies LECrim). Tras recordar su propia doctrina (recogida en las SSTs 342/2013, de 17 de abril y 493/2010, de 25 de abril), así como la fijada en las SSTs de la Sala Cuarta de lo Social de 26 de septiembre de 2007, 8 de marzo y 6 de octubre de 2011; aborda el análisis de las SSTC 241/2012, de 17 de diciembre, y 170/2013, de 7 de octubre, que contemplan supuestos similares, para, finalmente, asumir la doctrina *Barbulescu*. Para el Tribunal Supremo, no se trata de una doctrina «totalmente rupturista», en el sentido de que sus criterios son coincidentes con los que habían ido «cristalizando en nuestra jurisprudencia», pero admite que aportan y concretan «con diáfana claridad [los] parámetros de inexcusable respeto» para la resolución de este tipo de asuntos, que la Sala resume de la siguiente manera (FJ 10): «Si existiese esa expresa advertencia o instrucción en orden a la necesidad de limitar el uso del ordenador a tareas profesionales (de la que podría llegar a derivarse una anuencia tácita al control o, al menos, el conocimiento de esa potestad de supervisión) y/o además alguna cláusula conocida por ambas partes autorizando a la empresa a medidas como la aquí llevada a cabo; o, si se hubiese recabado previamente el consentimiento de quien venía usando de forma exclusiva el ordenador (en caso de negativa, nada impedía recabar la autorización necesaria) pocas dudas podrían albergarse sobre la legitimidad de la actuación indagatoria llevada a cabo por la empresa. Pero en las circunstancias en que se llevó a cabo hay que afirmar que el ordenamiento ni consiente, ni consentía en la fecha de los hechos, tal acción intrusiva por ser lesiva de derechos fundamentales». Para concluir que lo que «vicia la prueba es el

acceso no legítimo» (FJ 11), aclarando que la «muralla [de protección del derecho] solo cede en virtud del consentimiento del afectado o de autorización judicial», con independencia del contenido o del resultado concreto de lo encontrado. «La ilegitimidad de la medida [basada en un juicio *ex ante*] no deriva del contenido obtenido, ni de la forma de acceso más o menos intrusiva, sino del mismo acceso inconsentido y no advertido previamente». Como recuerda previamente esta misma sentencia, en frase ya reiterada: «los trabajadores no dejan ni su intimidad ni el resto de sus derechos en las puertas de la oficina o empresa» (FJ 3).

Afirmada la vulneración del derecho fundamental, el Tribunal Supremo aclara las consecuencias que puedan derivarse de lo anterior (FJ 13): «Primero, delimitar si tal actuación queda afectada por la prohibición contenida en el art. 11.1 LOPJ. En caso afirmativo, determinar si la supresión de las pruebas que han de ser invalidadas (en este caso los correos electrónicos o archivos extraídos de ese ordenador, así como las pruebas vinculadas a esa de una forma tan directa y jurídicamente relevante que pueda hablarse de una conexión de antijuricidad) nos arrastra a un vacío probatorio o, si, por el contrario, existen pruebas convalidables por ser desconectables o por emanar de fuentes independientes».

Para la Sala, aunque existen matices entre una vulneración causada por los poderes públicos y la causada por un particular, la inequívoca intención de «hacer valer como prueba, en su caso, los datos recabados» (FJ 14) y la existencia de «un cuerpo de doctrina que alertaba sobradamente sobre la dudosa legalidad» de la actuación empresarial (FJ 15) implican la nulidad de la prueba, *ex art.* 11.1 LOPJ.

A continuación, con remisión a la STS 299/2013, de 27 de febrero, se analizan los posibles efectos de esa declaración:

«a) Si la prueba indebidamente valorada por ser nula o ilícita era prescindible y puede asegurarse sin temor a equivocaciones que, suprimida, el pronunciamiento de condena no pierde sustento y hubiese sido el mismo se impondrá mantener la condena. [...]

b) Si la prueba anulada se revelaba como esencial, de forma que el fallo condenatorio al borrar esa prueba pierde todo o, al menos, su principal apoyo, habrá que proceder directamente a la absolución por aplicación de la presunción de inocencia. [...]

c) Solo cuando el marco probatorio sea lo suficientemente complejo como para no poder deducirse de forma indubitada qué influjo pudo tener la prueba anulada, es decir si era o no decisiva para fundamentar la convicción o se limitaba a corroborar lo que ya podía considerarse acreditado

por otros elementos, habrá que reenviar la causa al Tribunal *a quo*, para que dicte una nueva sentencia sin contar con esa prueba que se considera vulneradora de derechos fundamentales o para celebrar un nuevo juicio (sí se atisba pérdida de la imparcialidad en el Tribunal o el modelo de proceso —jurado— no consiente otra alternativa)».

En los casos en los que faltan elementos para llegar a una conclusión clara en uno u otro sentido, solo en esos, se deja abierta la cuestión para que de nuevo el órgano de la instancia adopte una nueva decisión sin contar con ese medio probatorio». Decisión que fue la finalmente adoptada en este caso.

3.2. *El análisis de los sistemas de grabación (la doctrina López Ribalda)*

La STEDH de 17 de octubre de 2019 (*asunto López Ribalda y otros c. España*) abordó un supuesto consistente en una eventual vulneración del art. 8 CEDH, derivada de la colocación de cámaras ocultas dirigidas a la zona de caja de un supermercado, para comprobar irregularidades de los trabajadores, y su uso con fines disciplinarios. También se alegaba la vulneración del art. 6 CEDH («proceso justo»), por utilización de estas imágenes como prueba en el juicio por despido.

Tras reiterar la doctrina del asunto *Barbulescu* (§§ 111, 112, 115, 116), el TEDH constata que, a diferencia del anterior, en el caso López Ribalda ya existía un marco legal regulador de este tipo de situaciones (integrado por la LO 15/1999, de 13 de diciembre, de Protección de Datos Personales; la Instrucción 1/2006 de la Agencia Española de Protección de Datos; el art. 20.3 del Estatuto de los Trabajadores; y las SSTC 186/2000, 29/2013 y 39/2016). Por tanto, el TEDH analiza la actuación de los tribunales nacionales bajo el prisma del cumplimiento de ese marco regulatorio.

Así, el tribunal europeo constata que las resoluciones entonces impugnadas realizaron una adecuada ponderación sobre los siguientes elementos valorativos:

- i) La legitimidad de la instalación del sistema de videovigilancia, basada en «la sospecha, alegada por el gerente del supermercado debido a las importantes pérdidas registradas durante varios meses, de que se habían cometido robos. También tuvieron en cuenta el interés legítimo del empleador en adoptar medidas para descubrir y castigar a los responsables de las pérdidas, con el fin

- de garantizar la protección de sus bienes y el buen funcionamiento de la empresa» (§ 123).
- ii) El «alcance de la vigilancia y el grado de intrusión en la vida privada de las demandantes», concluyendo que la medida era «limitada en cuanto a las zonas y el personal que se vigilaban —ya que las cámaras solo cubrían la zona de caja, que probablemente era donde se producían las pérdidas— y que su duración no había superado lo necesario para confirmar las sospechas de robo» (§ 124).
 - iii) Los distintos «lugares en los que se llevó a cabo la vigilancia, a la luz de la protección de la privacidad que un empleado podría razonablemente esperar. Esa expectativa es muy elevada en los lugares de carácter privado como los aseos o los vestuarios, en los que se justifica una mayor protección, o incluso la prohibición total de la videovigilancia [...]. Sigue siendo elevada en las zonas de trabajo cerradas, como las oficinas. Es manifiestamente inferior en los lugares visibles o accesibles a los compañeros o, como en el presente caso, al público en general» (§ 125).
 - iv) El «alcance de la medida en el tiempo», limitada al visionado del periodo necesario para identificar a los empleados responsables de la infracción (§ 126).
 - v) En cuanto a las «consecuencias de la vigilancia [...], no fueron utilizadas por el empleador para ningún otro fin que el de localizar a los responsables de las pérdidas registradas de bienes y adoptar medidas disciplinarias contra ellos» (§ 127).
 - vi) La necesidad de la medida, es decir, que «en las circunstancias del caso, no había ningún otro medio de cumplir el objetivo legítimo perseguido» (§ 128).
 - vii) El consentimiento previo del interesado no parece exigible en estos casos, lo que no excluye el deber de información sobre la existencia y condiciones de la recogida de datos, aunque solo sea de manera general. No obstante, la infracción del deber de información constituye «solo uno de los criterios que deben tenerse en cuenta», en el marco de una valoración conjunta del resto de elementos ponderativos, que adquieren una particular relevancia en el caso de que no se haya facilitado esa información (§ 131), ya que «solo un requisito primordial relativo a la protección de intereses públicos o privados importantes podría justificar la falta de información previa» (§ 133).

El TEDH concluyó que los tribunales habían verificado que la videovigilancia «estaba justificada por una finalidad legítima y [que] las medidas adoptadas a tal efecto eran adecuadas y proporcionadas, observando en particular que la finalidad legítima perseguida por el empleador no podía alcanzarse con medidas menos intrusivas para los derechos de las demandantes» (§ 132), máxime «teniendo en cuenta las importantes medidas que ofrece el marco jurídico español, incluidos los recursos que las demandantes no utilizaron, y el peso de las consideraciones que justifican la videovigilancia, tal como las han tenido en cuenta los tribunales nacionales» (§ 137), por lo que se rechazó la vulneración del art. 8 CEDH.

Otro tanto puede decirse de la alegada vulneración del art. 6 CEDH. El tribunal europeo, tras constatar que «las demandantes tuvieron acceso a las grabaciones obtenidas mediante la videovigilancia impugnada y pudieron impugnar su autenticidad y oponerse a su utilización como prueba» (§ 155), observa que la «principal queja se basaba en la falta de información previa sobre la instalación de las cámaras» (§ 156), lo que ya fue descartado como elemento decisivo para apreciar una vulneración del art. 8 CEDH. Y, en todo caso, «las grabaciones en cuestión no fueron las únicas pruebas en las que los tribunales nacionales basaron sus conclusiones» (§ 157), por lo que concluyó que «la utilización como prueba de las imágenes obtenidas por videovigilancia no menoscabó la equidad del procedimiento en el presente caso» (§ 158).

La doctrina *López Ribalda* ha sido expresamente acogida en la STC 119/2022, de 29 de septiembre, en la que, asumiendo anteriores pronunciamientos (SSTC 98/2000, de 10 de abril; 186/2000, de 10 de julio; 292/2000, de 30 de noviembre; 39/2016, de 3 de marzo; y 66/2022, de 2 de junio), se aborda un supuesto de régimen disciplinario laboral, consistente en la utilización del visionado de las grabaciones obtenidas del sistema de seguridad de la empresa como prueba para acreditar la causa del despido de un trabajador, motivado por la apropiación del dinero obtenido mediante la venta —por su cuenta— de productos de la empresa. En la STC 119/2022 se contiene una doctrina que puede ser de aplicación en otros ámbitos y que, por su interés, extractamos en sus elementos esenciales.

Así, respecto a la normativa aplicable, señala el Tribunal que, en el «ámbito concreto de las relaciones laborales, la LOPDGDD [Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales] ha previsto expresamente una serie de criterios generales para el tratamiento de los datos derivado del uso de dispositivos de

videovigilancia y de grabación de sonidos. Estos criterios se desprenden de la interpretación y aplicación conjunta de los arts. 22 y 89 LOPDGDD, en el marco general descrito en el art. 20 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, ET)» [FJ 5.b)].

Sobre la base de esa normativa, el Tribunal fija una doctrina que se concreta en una doble vertiente: sobre el derecho a la protección de datos personales (art. 18.4 CE) y sobre el derecho a la intimidad personal (art. 18.1 CE).

a) Sobre el derecho a la protección de datos

«El consentimiento del titular de los datos y el consiguiente deber de información sobre su tratamiento se configuran como elementos determinantes del contenido esencial del derecho a la protección de los datos personales reconocido en el art. 18.4 CE. Por lo que se refiere a la instalación de sistemas de videovigilancia y la utilización de las imágenes para fines de control laboral, el tratamiento de esos datos no exige el consentimiento expreso del trabajador, porque se entiende implícito por la mera relación contractual. Pero, en todo caso, subsiste el deber de información del empresario, como garantía ineludible del citado derecho fundamental. En principio, este deber ha de cumplimentarse de forma previa, expresa, clara y concisa. Sin embargo, la norma permite que, en caso de flagrancia de una conducta ilícita, el deber de información se tenga por efectuado mediante la colocación en lugar visible de un distintivo que advierta sobre la existencia del sistema, su responsable y los derechos derivados del tratamiento de los datos. El fundamento de esta excepción parece fácilmente deducible: no tendría sentido que la instalación de un sistema de seguridad en la empresa pudiera ser útil para verificar la comisión de infracciones por parte de terceros y, sin embargo, no pudiera utilizarse para la detección y sanción de conductas ilícitas cometidas en el seno de la propia empresa. Si cualquier persona es consciente de que el sistema de videovigilancia puede utilizarse en su contra, cualquier trabajador ha de ser consciente de lo mismo» [FJ 6.b)].

b) Sobre el derecho a la intimidad

«Como se deduce de nuestra doctrina y de los pronunciamientos del TEDH, para valorar si la colocación y utilización de un sistema de videovigilancia en una empresa con fines de control laboral puede afectar al derecho a la intimidad de los trabajadores se hace necesario realizar un juicio de pon-

deración, conforme al triple canon que, partiendo de la existencia de un fin legítimo, valore la idoneidad, necesidad y proporcionalidad de la medida.

El establecimiento de sistemas de control responde a una finalidad legítima en el marco de las relaciones laborales. Se trata de verificar el cumplimiento de los deberes inherentes a toda relación contractual. Así lo admite expresamente el art. 20.3 ET que, no obstante, establece como límite infranqueable la “consideración debida a [la] dignidad” del trabajador, lo que se complementa con el art. 20 bis ET, que reconoce a los trabajadores el “derecho a la intimidad [...] frente al uso de dispositivos de videovigilancia”. Por lo tanto, la mera constatación de un fin legítimo no excluye la debida ponderación sobre una eventual afectación de ese derecho.

En las concretas circunstancias del caso, puede afirmarse que la instalación del sistema de videovigilancia y la consiguiente utilización de las imágenes captadas resultaba una medida justificada, idónea, necesaria y proporcionada.

- i) La medida estaba justificada, porque concurrían sospechas indiciarias suficientes de una conducta irregular del trabajador [...] que debía ser verificada.
- ii) La medida puede considerarse como idónea para la finalidad pretendida, que no era otra que la constatación de la eventual ilicitud de la conducta, lo que fue confirmado precisamente mediante el visionado de las imágenes.
- iii) La medida era necesaria, ya que no parece que pudiera adoptarse ninguna otra menos invasiva e igualmente eficaz para acreditar la infracción laboral. Cualquier otra medida habría advertido al trabajador, haciendo entonces inútil la actuación de la empresa.
- iv) Finalmente, la medida puede considerarse como proporcionada. En este punto hay que ponderar diversos elementos de juicio. Así, en primer lugar, las cámaras no estaban instaladas en lugares de descanso, ocio o de carácter reservado, en los que existiera una expectativa razonable de privacidad, sino que estaban instaladas en zonas de trabajo abiertas a la atención al público. En segundo lugar, las cámaras no estaban instaladas de forma subrepticia, sino que estaban ubicadas en lugares visibles, tanto para los trabajadores del establecimiento como para el público en general. En tercer lugar, las cámaras no fueron utilizadas con carácter generalizado o indefinido, o para realizar una investigación de carácter prospectivo, sino para verificar la posible existencia de una conducta irregular detectada el día anterior. Por lo tanto, el grado de intromisión en la esfera de la intimidad del trabajador (art. 18.1 CE), en términos de espacio y tiempo, no puede considerarse como desequilibrado frente a los derechos e intereses de la empresa en la

detección y sanción de las conductas atentatorias contra la buena fe contractual, en el marco del ejercicio de los derechos a la propiedad privada y a la libertad de empresa, reconocidos en los arts. 33 y 38 CE, respectivamente.

Por todo ello, puede descartarse que se haya producido una lesión del derecho a la intimidad personal consagrado en el art. 18.1 CE» [FJ 6.c)].

4. Los derechos y las garantías en la investigación de hechos con relevancia penal

Como ya se expuso, la Ley 2/2023 no tiene por objeto principal la investigación de hechos delictivos. Sin embargo, los hechos denunciados o verificados tras la instrucción correspondiente pueden revestir carácter penal. Así se admite expresamente cuando se describe el ámbito material de esta norma [art. 2.1.b)].

En principio, la denuncia de un hecho que, inicialmente, presente una inequívoca naturaleza delictiva no debería plantear mayor problema en su tramitación, dado que, en ese caso, debe remitirse al Ministerio Fiscal [art. 9.2.j)]. Las cuestiones más problemáticas se pueden presentar cuando, en el marco de una denuncia por unos hechos que, de entrada, no parecen delictivos, aparecen con posterioridad indicios de un hecho con significación penal. O cuando, a pesar de la inicial apariencia delictiva, es necesario proceder a su depuración previa, tanto en la delimitación concreta de los hechos como de su posible autoría. Esta labor de desbroce no es propiamente una investigación penal en sentido estricto, entre otras cosas, porque no está dirigida por las autoridades competentes para ello: jueces, magistrados y fiscales (arts. 117 y 124 CE) o agentes policiales (art. 126 CE)²⁷.

Sin embargo, cabe preguntarse sobre el régimen jurídico aplicable a la práctica de estas diligencias, ante la eventualidad de su posterior utilización en un procedimiento de investigación penal.

²⁷ En este punto hay que señalar que el art. 19.4 de la Ley reconoce la consideración de «agentes de la autoridad» a los funcionarios de la Autoridad Independiente de Protección del Informante, AAI, que desarrollen actividades de investigación. No obstante, esta previsión, además de estar prevista exclusivamente en el ámbito de la AAI, no de las empresas, no implica su equiparación con los agentes policiales, sino más bien con los funcionarios públicos que han de estar revestidos de la autoridad necesaria para el ejercicio de potestades sancionadoras. (art. 30 del Real Decreto 33/1986, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado).

La Ley, como ya se indicó, adolece de una extraordinaria parquedad sobre estos aspectos que, a mi juicio, son de una enorme importancia. Pero esta escasez normativa no impide deducir algunos principios elementales que sirvan de guía para abordar el contenido de la investigación sin merma alguna de los derechos de las personas afectadas, tanto del denunciante (en su legítima pretensión de garantizar la regularidad de la obtención de las fuentes de prueba, como presupuesto para el ejercicio de una posterior acción penal) como del investigado (a fin de garantizar que cualquier actuación de investigación no suponga una merma de sus derechos fundamentales, sustantivos y procesales). En este apartado abordaremos algunas de las cuestiones que, a mi juicio, pueden presentar una mayor incidencia práctica.

a) El art. 39 reconoce los derechos a la presunción de inocencia y a la defensa de la persona investigada. Este precepto, aplicable a las investigaciones seguidas tanto en el ámbito público como privado, es objeto de varias concreciones a lo largo del texto, singularmente en su art. 9.2. Así, se reconoce el derecho a ser informado de los hechos que se le atribuyen y a ser oído en cualquier momento [apartado *f*)]; el derecho a la confidencialidad [apartado *g*)]; el derecho a la presunción de inocencia y al honor [apartado *h*)], y el derecho a la protección de datos personales [apartado *i*)].

A mi juicio, estas previsiones normativas constituyen una concreción de las garantías procesales que, configuradas como derechos fundamentales en el art. 24.2 CE, resultan de aplicación en el ámbito del derecho administrativo sancionador, y que el legislador ha querido extender a las investigaciones derivadas de la utilización de los sistemas internos o externos de información.

La aplicación de los principios del Derecho penal al ámbito del derecho administrativo sancionador es una tesis muy consolidada. La STC 18/1981, de 8 de junio (FJ 2), puso de manifiesto la íntima relación de identidad entre la naturaleza y los principios informadores de ambas potestades, como manifestaciones de un único *ius puniendi* del Estado. Así, tras admitir que el art. 24 CE no hace referencia expresa al ejercicio de la potestad sancionadora de la Administración, entiende no obstante que «los principios inspiradores del orden penal son de aplicación, con ciertos matices, al derecho administrativo sancionador, dado que ambos son manifestaciones del ordenamiento punitivo del Estado, tal y como refleja la propia Constitución (art. 25, principio de legalidad) y una muy reiterada jurisprudencia de nuestro Tribunal Supremo (Sentencia de la Sala

Cuarta de 29 de septiembre, 4 y 10 de noviembre de 1980, entre las más recientes), hasta el punto de que un mismo bien jurídico puede ser protegido por técnicas administrativas o penales». Más adelante aclara que «los principios esenciales reflejados en el art. 24 de la Constitución en materia de procedimiento han de ser aplicables a la actividad sancionadora de la Administración, en la medida necesaria para preservar los valores esenciales que se encuentran en la base del precepto, y la seguridad jurídica que garantiza el art. 9 de la Constitución. No se trata, por tanto, de una aplicación literal, [...] sino con el alcance que requiere la finalidad que justifica la previsión constitucional». Este principio general ha sido reiterado posteriormente en numerosas sentencias (entre otras, las SSTC 54/2003, de 24 de marzo; 226/2007, de 22 de octubre; 59/2014, de 5 de mayo, o la más reciente 93/2018, de 17 de septiembre). Y así se ha mantenido también, desde la perspectiva doctrinal, por diversos autores²⁸.

Eso supone que los arts. 24 y 25 CE reconocen un conjunto de garantías que se configuran como derechos fundamentales del ciudadano y que irradian su vigencia frente a la actuación de la administración y de la jurisdicción penal, al convertirse en límites a la potestad sancionadora del Estado. A tal efecto, puede citarse la STC 77/1983, de 3 de octubre (FJ 3), que señaló como límites de esa potestad sancionadora la legalidad, la interdicción de las penas de privación de libertad, el respeto de los derechos de defensa, y la subordinación a la Autoridad judicial. Doctrina que fue posteriormente reiterada, entre otras, en la STC 218/2013, de 19 de diciembre (FJ 4), con cita expresa de la STC 90/2010, de 7 de mayo (FJ 4) y de las SSTC 135/2010, de 2 de diciembre, y 144/2011, de 26 de septiembre. En estas resoluciones, el Tribunal afirma la vigencia de los principios de *nullum crimen nulla poena sine lege*, de aplicación al ordenamiento administrativo sancionador y que comprende una doble garantía, formal y material, que trae causa del mandato de taxatividad o de *lex certa* y se concreta en la exigencia de predeterminación normativa de las conductas ilícitas y de las sanciones correspondientes.

La aplicación de los principios del Derecho penal al derecho administrativo sancionador ha tenido un ámbito muy amplio en lo relativo a las

²⁸ Vid., entre otros, E. GARCÍA DE ENTERRÍA y T. R. FERNÁNDEZ RODRÍGUEZ, *Curso de Derecho Administrativo*, Madrid, 2015; R. PARADA, *Derecho Administrativo*, Madrid, 2017, o L. PAREJO AFONSO, *Lecciones de Derecho Administrativo*, Valencia, 2018. Aunque no faltan otros autores que propugnan la autonomía del derecho administrativo sancionador, señaladamente, A. NIETO GARCÍA, que en su *Derecho administrativo sancionador*, Madrid, 2012, pone en duda la existencia de un único *ius puniendi* del Estado.

garantías procedimentales. Así nos lo recuerda la STC 59/2014, de 5 de mayo (FJ 3), cuando señala que «se ha ido elaborando progresivamente una doctrina que asume la vigencia en el seno del procedimiento administrativo sancionador de un amplio abanico de garantías del art. 24 CE. Sin ánimo de exhaustividad, se pueden citar el derecho a la defensa, que proscribire cualquier indefensión; el derecho a la asistencia letrada, trasladable con ciertas condiciones; el derecho a ser informado de la acusación, con la ineludible consecuencia de la inalterabilidad de los hechos imputados; el derecho a la presunción de inocencia, que implica que la carga de la prueba de los hechos constitutivos de la infracción recaiga sobre la Administración, con la prohibición de la utilización de pruebas obtenidas con vulneración de derechos fundamentales; el derecho a no declarar contra sí mismo; y, en fin, el derecho a utilizar los medios de prueba adecuados para la defensa, del que se deriva que vulnera el art. 24.2 CE la denegación inmotivada de medios de prueba [por todas, SSTC 7/1998, de 13 de enero, FJ 5; 3/1999, de 25 de enero, FJ 4, y 14/1999, de 22 de febrero, FJ 3.a); 276/2000, de 16 de noviembre, FJ 7, y 117/2002, de 20 de mayo, FJ 5]».

Aunque las investigaciones derivadas de la Ley del informante no pueden ser equiparadas, sin más, con la potestad administrativa sancionadora ni, mucho menos, con el ejercicio del *ius puniendi* del Estado en materia penal (que, en su caso, serán exigibles a partir del resultado de la investigación interna), un elemental principio de interpretación integradora del ordenamiento jurídico podría permitir que los principios y garantías ya expuestos estuvieran presentes, con las modulaciones correspondientes, en el ámbito de las investigaciones internas previstas en la norma, como seguidamente veremos.

b) En efecto, conviene recordar que el derecho fundamental a la presunción de inocencia (art. 24.2 CE) presenta dos vertientes: una interna o procesal y otra externa o extraprocesal.

Así, en su vertiente interna o como regla de juicio, la STC 111/1999, de 14 de junio (FJ 2) señala que este derecho «sirve de base a todo el procedimiento criminal y condiciona su estructura» (STC 56/1982), constituyendo «uno de los principios cardinales del Derecho penal contemporáneo, en sus facetas sustantiva y formal» (SSTC 138/1992, 133/1995), por cuanto beneficia únicamente al acusado y le otorga toda una serie de garantías específicas en cada estadio de desarrollo del proceso (STC 41/1997, fundamento jurídico 5.º). Entre otros contenidos, que hemos recordado en el ATC 214/1998, este derecho no permite una condena sin pruebas, lo que hace referencia a la presunción de inocencia en su dimensión de regla de

juicio y supone que cuando el Estado ejercita el *ius puniendi* a través de un proceso, debe estar en condiciones de acreditar públicamente que la condena se ha impuesto tras la demostración razonada de que el acusado ha cometido realmente el concreto delito que se le atribuía, a fin de evitar toda sospecha de actuación arbitraria. En este sentido, toda Sentencia condenatoria debe estar sustentada en pruebas de cargo válidas, validez que implica no solo la conformidad a la Ley de Enjuiciamiento Criminal, sino además la conformidad de estas a la propia Constitución, correspondiendo la carga de la prueba a quien acusa.

La definición de la presunción de inocencia, que desde la perspectiva constitucional debe entenderse como «derecho a no ser condenado sin pruebas de cargo válidas» (STC 81/1998, fundamento jurídico 3.º), implica que es la sentencia condenatoria la que debe expresar las pruebas de cargo que sustentan la declaración de responsabilidad jurídico-penal, que a su vez deben proceder de actos de prueba conformes a la Ley y a la Constitución y normalmente practicados en el acto del juicio oral, con todas las garantías. En relación con esta previa actividad probatoria, se exigió en un primer momento, a partir de la fundamental STC 31/1981, que fuera «mínima», después, desde la STC 109/1986, que resultase «suficiente», y últimamente hemos requerido que el fallo condenatorio se apoye en «verdaderos» actos de prueba (por ejemplo, SSTC 150/1989, 201/1989, 131/1997, 173/1997, 41/1998 y 68/1998).

El derecho a la presunción de inocencia como regla de juicio «impone exigencias tanto respecto a quién debe aportar las pruebas, en qué momento y lugar deben practicarse los medios de prueba, qué debe entenderse por prueba legal y constitucionalmente válida, como respecto a la necesidad de que la valoración probatoria se someta a las reglas de la lógica y de la experiencia (SSTC 94/1990 y 115/1998), así como a la obligación de motivar (SSTC 44/1987, 22/1988 fundamento jurídico 4.º; 160/1988, 44/1989; 138/1990; 259/1994 fundamento jurídico 2.º, *in fine*; 153/1997; 47/1998; 49/1998, y 115/1998) o razonar el resultado de la valoración probatoria [SSTC 182/1989; 76/1990 fundamento jurídico 8.º.B); 41/991; 102/1994; 45/1997; 123/1997]».

En su vertiente externa o como regla de tratamiento, la STC 91/2021, de 21 de abril (FJ 8.3) la define como «el derecho a recibir la consideración y el trato de no autor o no partícipe en hechos de carácter delictivo o análogo a estos, sin previa resolución dictada por el poder público u órgano competente que así lo declare, y determina por ende el derecho a que no se apliquen las consecuencias o los efectos jurídicos anudados a hechos

de tal naturaleza en las relaciones jurídicas de todo tipo» [STC 109/1986, de 24 de septiembre, FJ 1; seguida por SSTC 283/1994, de 24 de octubre, FJ 2; 166/1995, de 20 de noviembre, FJ 3; 244/2007, de 10 de diciembre, FJ 2, y 133/2018, de 13 de diciembre, FJ 4.a)].

Como recordó el Pleno en la citada STC 133/2018, «[e]ste tribunal ha considerado que la dimensión extraprocesal de la presunción de inocencia, reconocida también por el Tribunal Europeo de Derechos Humanos en el marco del art. 6.2 CEDH (SSTEDH, de 10 de febrero de 1995, asunto *Allenet de Ribemont c. Francia*; de 26 de marzo de 2002, asunto *Butkevicius c. Lituania*; de 28 de junio de 2011, asunto *Lizaso Azconobieta c. España*), encuentra específica protección en nuestro sistema de derechos fundamentales a través o por medio de la tutela del derecho al honor, operando dicha presunción como elemento instrumental del enjuiciamiento de una posible lesión del derecho al honor (STC 244/2007, FJ 2). [...] “[E]sta dimensión extraprocesal de la presunción de inocencia, no constituye por sí misma un derecho fundamental distinto o autónomo del que emana de los arts. 10 y 18 de la Constitución, de tal modo que ha de ser la vulneración de estos preceptos, y señaladamente del art. 18, lo que sirva de base a su protección a través del recurso de amparo, [p]orque [...] la presunción de inocencia que garantiza el art. 24.2 CE, alcanza el valor de derecho fundamental susceptible de amparo constitucional, cuando el imputado en un proceso penal, que ha de considerarse inocente en tanto no se pruebe su culpabilidad, resulte condenado sin que las pruebas, obtenidas y practicadas con todas las garantías legal y constitucionalmente exigibles, permitan destruir dicha presunción. En los demás casos relativos al honor y a la dignidad de la persona, que no son una presunción sino una cualidad consustancial inherente a la misma, serán los derechos consagrados en el art. 18 CE los que, por la vía del recurso de amparo, habrán de ser preservados o restablecidos” (STC 166/1995, FJ 3; doctrina que reitera la STC 244/2007, FJ 2)» [STC 133/2018, FJ 4.a)].

Estas dos vertientes resultan de especial interés en el ámbito que analizamos. No solo porque, como es lógico, se habrá de entender que no existirá responsabilidad de tipo alguno (laboral, administrativa o penal) hasta que se demuestre fehacientemente lo contrario por parte de quien la atribuye; sino porque la autoridad pública o privada competente para la investigación de la denuncia interna habrá de tener por inocente, a todos los efectos, a la persona denunciada, sin que pueda adoptarse medida alguna de la que pudiera derivarse la consideración de responsable de una infracción laboral, administrativa o delictiva, medidas que solo serían proceden-

tes en el marco de un ulterior procedimiento, conforme a los presupuestos y requisitos establecidos en la legislación correspondiente²⁹.

c) Sobre el derecho de defensa existe una consolidada doctrina del Tribunal Constitucional, recientemente recordada en la STC 29/2023, de 17 de abril (FJ 2).

Así, el «derecho fundamental a obtener la tutela judicial efectiva, reconocido en el art. 24.1 CE, comporta la exigencia de que en ningún momento pueda producirse indefensión, lo que, puesto en relación con el reconocimiento del derecho de defensa, en el apartado 2 del mismo precepto constitucional, [...] significa que en todo proceso judicial debe respetarse el derecho de defensa contradictoria de las partes contendientes (SSTC 143/2001, de 18 de junio, FJ 3; 93/2005, de 18 de abril, FJ 3; 12/2006, de 16 de enero, FJ 3; 13/2006, de 16 de enero, FJ 4, y 65/2007, de 27 de marzo, FJ 2).

La posibilidad de defensa contradictoria es, por tanto, una de las reglas esenciales del desarrollo del proceso, sin cuya concurrencia, debemos reiterar, la idea de juicio justo es una simple quimera. Se trata de un derecho formal cuyo reconocimiento no depende de la calidad de la defensa que se hubiera llegado a ejercer (SSTC 93/2005, FJ 3; 12/2006, FJ 3; 61/2007, de 26 de marzo, FJ 2, y 65/2007, FJ 2) [...].

La obligación del órgano jurisdiccional de garantizar la defensa contradictoria es exigible tanto cuando las partes comparezcan por sí mismas, [...] como cuando lo hagan con la asistencia de letrado, si optaren por esta posibilidad, o la misma fuere legal —y añadimos, constitucionalmente— impuesta (SSTC 93/2005, FJ 3; 12/2006, FJ 3, y 13/2006, FJ 4) [...].

También hemos destacado, que son manifestaciones específicas del derecho de defensa las facultades de alegar, probar e intervenir en la prueba ajena para controlar su correcta práctica y contradecirla y muy concretamente la de “interrogar o hacer interrogar a los testigos que declaren contra él”, facultad esta que el art. 6.3.d) del Convenio europeo de derechos humanos reconoce a todo acusado como regla general entre sus mínimos derechos; y de un tenor similar es el art. 14.3.e) del Pacto internacional de derechos civiles y políticos. (SSTC 143/2001, FJ 3; 93/2005, FJ 3; 12/2006, FJ 3; 13/2006, FJ 4, y 65/2007, FJ 2)».

Esta doctrina, prevista para un procedimiento judicial, puede ser trasladada, con las debidas matizaciones derivadas de su diferente naturaleza,

²⁹ *Vid.*, en tal sentido, lo dispuesto en el art. 36.6 de la Ley 2/2023.

a la investigación de una denuncia interna. Así parece deducirse de la propia norma. Por un lado, la persona denunciada habrá de ser informada de los hechos que se le atribuyen, podrá acceder al expediente y podrá aportar o proponer prueba (art. 19, apartados 2 y 3). Pero no podrá conocer la identidad del denunciante y, por el mismo motivo, tampoco podrá asistir a su declaración ni, mucho menos, interrogarla, precisamente para salvaguardar el derecho de esta a la confidencialidad y preservación de sus datos de identidad (art. 33) como presupuestos para la garantía de indemnidad que la propia Ley pretende proteger (art. 36). Por su parte, el denunciante podrá aportar, lógicamente, los medios de prueba de que disponga o proponer medios de prueba. También podrá ser requerido para aportar información adicional [art. 9.2.e)], y conocer el estado de la tramitación de su denuncia y los resultados de la investigación (art. 21-8.º).

d) El derecho de defensa debe ser distinguido del derecho a la asistencia letrada.

Conforme señala la STC 29/2023, de 17 de abril (FJ 3), ya citada, toda persona tiene derecho a la defensa, pero no necesariamente a la asistencia técnica o letrada, que puede ser preceptiva o potestativa. «En el supuesto en que la intervención de letrado sea preceptiva, esta garantía constitucional, además de un derecho, se convierte en una exigencia estructural del proceso tendente a asegurar su correcto desenvolvimiento, cuyo sentido es satisfacer el fin común a toda asistencia letrada, así como lograr el adecuado desarrollo del proceso, como mecanismo instrumental introducido por el legislador con miras a una dialéctica procesal efectiva, que facilite al órgano judicial la búsqueda de una sentencia ajustada a Derecho. [...] Ahora bien, en los supuestos en que la intervención de letrado no sea legalmente preceptiva la garantía de la asistencia letrada no decae como derecho fundamental de la parte procesal. A este respecto ha de tenerse en cuenta que, como derecho de la parte, el hecho de poder comparecer personalmente ante el juez o tribunal no obliga a las partes a actuar personalmente, sino que les faculta para elegir entre la autodefensa o la defensa técnica, dejándose a su libre disposición la opción por una u otra (SSTC 199/2003, FJ 5, y 65/2007, FJ 4). [...] Sin embargo, la exigencia legal de postulación, esto es, su carácter preceptivo, no coincide siempre con la necesidad constitucional de asistencia letrada. La necesidad constitucional de asistencia letrada viene determinada por la finalidad que este derecho cumple [SSTC 233/1998, de 1 de diciembre, FJ 3.B), y 225/2007, FJ 4]. Esto es, asentada la premisa de naturaleza constitucional, que sobre

el órgano jurisdiccional recae el deber de garantizar la igualdad de las partes y la efectiva contradicción para el correcto desarrollo del debate procesal, será constitucionalmente obligada la asistencia letrada allí donde la capacidad del interesado, el objeto del proceso, su dificultad técnica, la mayor o menor complejidad del debate procesal y la cultura y conocimientos jurídicos del comparecido personalmente, deducidos de la forma y nivel técnico con que haya realizado su defensa, hagan estéril la autodefensa que el mismo puede ejercer mediante su comparecencia personal (por todas, STC 47/1987, de 22 de abril, FJ 3), por más que la asistencia técnica carezca del preceptivo carácter legal».

La Ley 2/2023 solo contempla la asistencia letrada en el caso de las actuaciones llevadas a cabo por la Autoridad Independiente de Protección del Informante, AAI. Los arts. 19.3 y 21-5.º recogen la posibilidad de que tanto la persona denunciada como el informante, respectivamente, puedan comparecer asistidos de un abogado, y así habrán de ser informados. Se trata, en cualquier caso, de una norma potestativa, no imperativa. No es obligatorio que las partes acudan asistidas por un abogado. La norma no reconoce el derecho a la asistencia jurídica gratuita³⁰, por lo que cualquier actuación letrada habrá de ser costeada por las partes.

La regulación legal parece reducir la asistencia letrada al momento de prestar declaración. El denunciante y el denunciado podrían estar asistidos por los abogados de su elección respectivos en esas diligencias que les afectan con carácter personalísimo. Pero no parece tan clara la asistencia letrada respecto de la práctica del resto de las diligencias (por ejemplo, mediante la intervención en el interrogatorio de un testigo o en un examen pericial) ya que eso requeriría, a mi juicio, un reconocimiento del derecho a la personación que, como tal, no está previsto en la norma.

Nada se dice expresamente sobre las investigaciones llevadas a cabo en el ámbito de una empresa privada. No obstante, el art. 9.1 de la Ley establece, como disposición general³¹, que el «órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley aprobará

³⁰ La Ley 2/2023 solo contempla el derecho a la asistencia jurídica gratuita para los denunciantes, y únicamente en los procedimientos seguidos en cualquier orden jurisdiccional que sean consecuencia directa de la infracción comunicada, es decir, no durante la investigación de la denuncia interna, según establece la Disposición final primera, que modifica el art. 2 de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, añadiendo un apartado *k*) a tal efecto.

³¹ Así se deduce también de lo dispuesto en el art. 5.2, *f*) de la Ley, que obliga a respetar las garantías establecidas en el art. 9, «en cualquiera de [las] fórmulas de gestión» del sistema interno de información.

el procedimiento de gestión de informaciones», y el art. 9.2 señala que este procedimiento habrá de cumplir con los «requisitos establecidos en esta ley» y, en particular, habrá de respetar el «contenido mínimo» que se describe en el propio art. 9.2, en cuyo apartado *f*) se señala el derecho de la persona afectada (denunciada) a ser informada de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento. Aunque esta previsión legal no contempla expresamente la asistencia letrada, una interpretación integradora de la norma y coherente con la mayor efectividad del derecho de defensa, permitiría considerar que esa audiencia al denunciado podrá revestir las garantías propias de la instrucción llevada a cabo por la AAI, posibilitando la asistencia letrada —siempre con carácter facultativo— en las normas internas que regulen las investigaciones en el ámbito privado.

e) Finalmente, una vez analizado el conjunto de derechos y obligaciones de los intervinientes y algunas de las diligencias que puedan desarrollarse en el marco de las investigaciones internas, interesa destacar que, en todo caso, la utilidad de lo actuado en un ulterior proceso penal requerirá su aportación, reproducción o ratificación en presencia judicial.

Como recuerda la reciente STC 59/2023, de 23 de mayo (FJ 4), en un caso relativo a la validez de las actuaciones practicadas en el marco de unas diligencias de investigación del Ministerio Fiscal, «únicamente pueden considerarse auténticas pruebas que vinculen a los órganos de la justicia penal en el momento de dictar sentencia las practicadas en el juicio oral, pues es en este donde se aseguran las garantías constitucionales de inmediación, contradicción, oralidad y publicidad con fines de valoración probatoria (entre otras muchas, SSTC 182/1989, de 3 de noviembre, FJ 2; 67/2001, de 17 de marzo, FJ 6; 195/2002, de 28 de octubre, FJ 2; 206/2003, de 1 de diciembre, FJ 2; 345/2006, de 11 de diciembre, FJ 3; 68/2010, de 18 de octubre, FJ 5; 134/2010, de 2 de diciembre, FJ 3, y 53/2013, de 28 de febrero, FJ 3)». Y, aunque se admite la eficacia probatoria de algunas diligencias practicadas en fases anteriores del procedimiento, su validez se hace depender de que hayan sido llevadas a cabo «con las formalidades que la Constitución y el ordenamiento procesal establecen, siempre que hayan sido traídas al juicio oral y en condiciones que permitan a la defensa del acusado someterlas a contradicción [SSTC 80/1986, de 17 de junio, FJ 1; 187/2003, de 27 de octubre, FJ 3; 344/2006, de 11 de diciembre, FJ 4.*b*); 68/2010, de 18 de octubre, FJ 5, y 134/2010, de 2 de diciembre, FJ 3, entre otras]». En concreto, y como supuesto paradigmático, «la validez como prueba de cargo preconstitui-

da de las declaraciones prestadas en fase sumarial se condiciona al cumplimiento de una serie de requisitos, que este tribunal viene clasificando en materiales (imposible reproducción en el acto del juicio oral); subjetivos (necesaria intervención del juez de instrucción); objetivos (que se garantice la posibilidad de contradicción y la asistencia letrada al imputado, a fin de que pueda interrogar al testigo o perito); y formales (introducción del contenido de la declaración sumarial a través de la lectura del acta en que se documenta, conforme al art. 730 LECrim, o a través de los interrogatorios), lo que posibilita que su contenido acceda al debate procesal público ante el juez o tribunal sentenciador y se someta allí a contradicción y confrontación con las demás declaraciones de quienes sí intervinieron en el juicio oral (entre otras, SSTC 80/1986, de 17 de junio, FJ 1; 303/1993, de 25 de octubre, FJ 3; 40/1997, de 27 de febrero, FJ 2; 195/2002, de 28 de octubre, FJ 2; 187/2003, de 27 de octubre, FJ 3; 280/2005, de 7 de noviembre, FJ 2; 344/2006, de 11 de diciembre, FJ 4; 29/2008, de 20 de febrero, FJ 5, y 165/2014, de 8 de octubre, FJ 2)».

No parece que las diligencias practicadas en el marco de una investigación interna en el seno de una entidad pública o privada respondan a los parámetros propios de una prueba anticipada o preconstituída, entre otros motivos, porque no se practican ante un Juez ni con garantías de contradicción efectiva. Cuestión distinta es la obtención previa de fuentes de prueba que, como ya hemos visto en los ejemplos analizados en los apartados III.3.1 y III.3.2, habrán de recabarse de forma compatible con la protección de los derechos fundamentales en presencia, a fin de que puedan surtir efecto en el ulterior proceso. Lo relevante, en todo caso, es que no puede haber prueba alguna susceptible de ponderación que no haya sido aportada, reiterada, reproducida o practicada en el marco de un procedimiento judicial, y conforme a los principios de inmediación, contradicción, oralidad y publicidad. Por tanto, como regla general, las actuaciones llevadas a cabo en el marco del sistema interno de información habrán de ser ratificadas judicialmente, y solo en esa medida puede decirse que surtirán efecto en el eventual proceso judicial posterior.

IV. BIBLIOGRAFIA

a) Bibliografía de interés sobre la Ley y la figura del informante

BACHMAIER WINTER, L., «*Whistleblowing* europeo y *compliance*: La Directiva EU de 2019 relativa a la protección de personas que reporten infracciones del

- Derecho de la Unión», *Diario La Ley*, núm. 9.527 (2019), sección Tribuna, 27 de noviembre.
- DE ROS RAVENTÓS, I., «La investigación interna, la colaboración con las autoridades y la reparación del daño como causa de exención de la responsabilidad penal de la persona jurídica: una propuesta de modificación del art. 31 quáter», *La Ley compliance penal*, núm. 11 (2022).
- GARCÍA-PANASCO MORALES, G., «La nueva Ley del informante: cuando las buenas intenciones se pueden convertir en un problema», *Diario La Ley*, núm. 10.264 (2023), sección Tribuna, 11 de abril.
- GÓMEZ ASENSIO, J. A., «Regulación de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción», *Diario La Ley*, núm. 10.356 (2023), sección Tribuna, 26 de septiembre.
- LIÑÁN LAFUENTE, A., «La Ley 2/2023, de protección del informante, vs. el derecho de no auto incriminación de la persona jurídica», *La Ley Penal: Revista de Derecho penal, procesal y penitenciario*, núm. 162 (2023), ejemplar dedicado a: «Lobbies y corrupción pública».
- RAGUÉS I VALLÉS, R., «La Ley 2/2023 de protección de informantes: una primera valoración crítica», *La Ley compliance penal*, núm. 13 (2023).
- VILLEGAS GARCÍA, M.^a de los Á., y ENCINAR DEL POZO, M. Á., «Compliance, protección del informante e investigaciones internas», en C. GÓMEZ-JARA DÍEZ (coord.), *Persuadir y Razonar: Estudios Jurídicos en Homenaje a José Manuel Maza Martín*, Cizur Menor, Aranzadi, 2018, pp. 211-251.

b) Bibliografía de interés sobre la responsabilidad penal de las personas jurídicas y los programas de *compliance*

- ARROYO ZAPATERO, L., y NIETO MARTÍN, A. (dirs.), *El Derecho penal económico en la era compliance*, Valencia, Tirant lo Blanch, Teoría, 2013.
- BACIGALUPO ZAPATER, E., *Compliance y Derecho penal*, Cizur Menor, Thomson Reuters Aranzadi, 2011.
- BACIGALUPO SAGESSE, S., «Posición de garante del órgano de control y supervisión de riesgos penales en el ámbito societario. Sobre la función del *compliance officer*, su responsabilidad, independencia y facultades de investigación», *Diario La Ley*, núm. 9.632 (2020), sección Tribuna, 14 de mayo.
- BAJO FERNÁNDEZ, M.; FEIJOO SÁNCHEZ, B. J., y GÓMEZ-JARA DÍEZ, C., *Tratado de responsabilidad penal de las personas jurídicas*, Madrid, Civitas, 2016.
- BUXÓ OLIVÉ, J., y GÓMEZ I CASALTA, G., «Sobre la configuración de un Sistema de *Compliance*: algunas variables a tener en consideración», *La Ley compliance penal*, núm. 9 (2022).
- DE ÁNGEL YÁGÜEZ, R., *La doctrina del «levantamiento del velo» de la persona jurídica en la jurisprudencia*, 7.^a ed., Madrid, Civitas, 2017.
- DE LA CUERDA MARTÍN, M., «El asesor fiscal y su responsabilidad como autor de un delito fiscal vía art. 31 CP: ¿Es posible la admisión de una representación de hecho?», *La Ley compliance penal*, núm. 11 (2022).

- DE LA CUESTA ARZAMENDI, J. L. (dir.), y DE LA MATA BARRANCO, N. J. (coord.), *Responsabilidad penal de las personas jurídicas*, Cizur Menor, Thomson Reuters Aranzadi, 2013.
- DEL MORAL GARCÍA, A., «Responsabilidad penal de personas jurídicas: Notas con ocasión de la reforma de 2015», *Revista del Ministerio Fiscal*, núm. 0 (2015), pp. 215 y ss., disponible en *www.fiscal.es*, sección documentos.
- FISCALÍA GENERAL DEL ESTADO, Circulares núms. 1/2011, de 1 de junio, y 1/2016, de 22 de enero; sobre la responsabilidad penal de las personas jurídicas conforme a las reformas del Código Penal efectuadas, respectivamente, por las LO 5/2010 y 1/2015, disponibles en *www.fiscal.es*, sección documentos.
- *La responsabilidad penal de las personas jurídicas. Libro Homenaje al Excmo. Sr. Don José Manuel Maza Martín*, Madrid, Fiscalía General del Estado, 2018.
- GARCÍA-PANASCO MORALES, G., «El sistema vicarial y la carga de la prueba sobre los programas de *compliance* en la responsabilidad penal de las personas jurídicas: hacia la superación de un desencuentro», *Diario La Ley*, núm. 9.221 (2018), sección Documento on-line, 19 de junio.
- «La responsabilidad penal de las personas jurídicas: algunas cuestiones sobre el *compliance* y la protección de datos», *Revista La Ley Mercantil*, núm. 55 (2019).
- GÓMEZ-JARA, C., «Delito corporativo y responsabilidad penal de las personas jurídicas: un desarrollo coherente de la jurisprudencia del Tribunal Supremo», *Diario La Ley*, núm. 8.830 (2016), sección Doctrina, 23 de septiembre.
- *El Tribunal Supremo ante la Responsabilidad Penal de las Personas Jurídicas. El inicio de una larga andadura*, Cizur Menor, Thomson-Reuters Aranzadi, 2017.
- GÓMEZ TOMILLO, M., *Introducción a la responsabilidad penal en las personas jurídicas*, Cizur Menor, Thomson-Reuters Aranzadi, 2015.
- «Responsabilidad penal de las personas jurídicas y carga de la prueba de la idoneidad de los programas de cumplimiento», *Diario La Ley*, núm. 8.861 (2016), sección Tribuna, 11 de noviembre.
- GONZÁLEZ-CUÉLLAR SERRANO, N., y JUANES PECES, E., «La responsabilidad penal de las personas jurídicas y su enjuiciamiento en la reforma de 2010. Medidas a adoptar antes de su entrada en vigor», *Diario La Ley*, núm. 7.501 (2010), 3 de noviembre.
- GONZÁLEZ CUSSAC, J. L., «Responsabilidad penal de las personas jurídicas: arts. 31 bis, ter, quáter y quinquies», en J. L. GONZÁLEZ CUSSAC (dir.), *Comentarios a la Reforma del Código Penal de 2015*, Valencia, Tirant lo Blanch, 2015.
- KUHLEN, L.; MONTIEL, J. P., y ORTIZ DE URBINA GIMENO, Í. (coords.), *Compliance y teoría del Derecho penal*, Madrid, Marcial Pons, 2013.
- MAGRO SERVET, V., «Viabilidad de la pericial de *compliance* para validar la suficiencia del programa de cumplimiento normativo por las personas jurídicas», *Revista Diario La Ley*, núm. 9.337 (2019), sección Doctrina, 15 de enero.

- MAZA MARTÍN, J. M., *Delincuencia electoral y responsabilidad penal de los partidos políticos*, Madrid, Wolters Kluwer, 2018.
- MIR PUIG, S.; CORCOY BIDAOSLO, M.; GÓMEZ MARTÍN, V. (dirs.); HORTAL IBARRA, J. C., y VALIENTE IVÁNEZ, V. (coords.), *Responsabilidad de la empresa y compliance*, Madrid, Edisofer, 2014.
- MORILLAS CUEVA, L., «La cuestión de la responsabilidad penal de las personas jurídicas», *Revista Anales de Derecho*, núm. 29 (2011).
- NIETO MARTÍN, A., y MAROTO CALATAYUD, M. (dirs.), *Public compliance. Prevención de la corrupción en administraciones públicas y partidos políticos*, Cuenca, Universidad de Castilla-La Mancha, 2014.
- LASCURÁIN SÁNCHEZ, J. A., «Análisis de riesgos penales: cuatro inquietudes», *La Ley compliance penal*, núm. 7 (2021).
- PUYOL, J., *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*, con la colaboración de Lucía do Nascimento, Valencia, Tirant lo Blanch, 2018.
- QUINTERO OLIVARES, G., «La reforma del régimen de responsabilidad de las personas jurídicas», en G. QUINTERO OLIVARES (coord.), *La reforma penal de 2015*, Cizur Menor, Thomson-Reuters Aranzadi, 2015.
- RODRÍGUEZ RAMOS, L., «Sobre la culpabilidad de las personas jurídicas (al hilo de las SSTs 514/2015, 154 y 221/2016)», *Diario La Ley*, núm. 8.766 (2016), sección Doctrina, 20 de mayo.
- RUANO MOCHALES, T., «El administrador de la sociedad de capital frente a la responsabilidad penal de la persona jurídica y el *compliance*», *La Ley Mercantil*, núm. 43 (2018), sección Sociedades, enero.
- «Algunos interrogantes sobre la responsabilidad penal de las personas jurídicas», en J. SÁNCHEZ MELGAR (coord.) *et al.*, *Revista Práctica Penal*, núm. 86 (2017), 1.º trimestre.
- SÁNCHEZ MELGAR, J., «Los títulos de imputación de responsabilidad penal de las personas jurídicas, tras la reforma penal de 2015», *Revista Práctica Penal*, núm. 79 (2015), 2.º semestre.
- «La carga de la prueba en materia de responsabilidad penal de las personas jurídicas: de la cuadratura del círculo a la reconciliación», *Revista Práctica Penal*, núm. 87 (2017), 2.º trimestre.
- SILVA SÁNCHEZ, J. M.^a (dir.), y MONTANER FERNÁNDEZ, R. (coord.), *Criminalidad de empresa y compliance. Prevención y reacciones corporativas*, Barcelona, Atelier, 2013.
- VILLEGAS GARCÍA, M.^a Á., y ENCINAR DEL POZO, M. Á., «La responsabilidad penal de las personas jurídicas. La Jurisprudencia de la Sala de lo Penal del Tribunal Supremo», *Diario La Ley*, núm. 9.106 (2017), sección Dossier, 26 de diciembre.
- ZUGALDÍA ESPINAR, J. M., *La responsabilidad penal de empresas, fundaciones y asociaciones*, Valencia, Tirant lo Blanch, 2008.
- *La responsabilidad criminal de las personas jurídicas, de los entes sin personalidad y de sus directivos (Análisis de los arts. 31 bis y 129 del Código Penal)*, Valencia, Tirant lo Blanch, 2013.

ZUGALDÍA ESPINAR, J. M., y MARÍN DE ESPINOSA CEBALLOS, E. B. (coords.), *Aspectos prácticos de la responsabilidad criminal de las personas jurídicas*, Cizur Menor, Thomson Reuters Aranzadi, 2013.

— *La responsabilidad criminal de las personas jurídicas en Latinoamérica y en España*, Cizur Menor, Thomson Reuters Aranzadi, 2015.