MOLINS

Defensa Penal

Departamento de Investigaciones Internas

Anuario 2023

Recopilación de los principales hitos normativos y jurisprudenciales del año en materia de investigaciones internas

Índice

1. Comunidad internacional

A) Normativa

- **Guía de Investigaciones Internas en Organizaciones (ISO/TS 37008:2023).**

La principal novedad del año 2023 en el plano internacional fue la publicación de la Guía de Investigaciones Internas en Organizaciones (ISO/TS 37008:2023). Consiste en una guía para la conducción de investigaciones internas en cualquier tipo de organización.

El estándar llegó tras la trasposición de la Directiva (UE) 2019/1937, sobre protección de los informantes (*whistleblowers*), en la mayor parte de los países de la Unión. El proceso se ha prolongado más de lo esperable (el plazo concedido a los Estados miembros era de dos años), con tres retrasos destacables: España (febrero de 2023), Italia (marzo de 2023) y Alemania (junio de 2023). Estonia y Polonia siguen sin cumplir con el mandato de trasposición[1].

La guía aporta algo de luz en un ámbito hasta ahora carente de referentes normativos. Si bien las normas de trasposición de la Directiva (UE) 2019/1937 regulan algunos aspectos de las investigaciones internas, especialmente los relativos a la recepción y tramitación de las denuncias, la mayor parte del procedimiento sigue huérfano de ordenación legal, al menos en España. En nuestra **Ley n.º 2/2023**, de 20 de febrero, destaca la exigua regulación del procedimiento de investigación en las entidades privadas (*vid*. arts. 10 a 12), lo que contrasta con lo previsto en relación con las investigaciones llevadas a cabo por la autoridad independiente (*vid*. arts. 16 a 24).

De ahí que la publicación de este estándar internacional sea muy bienvenida. La principal aportación de la ISO 37008 es la de ofrecer un esquema completo de las diferentes fases y aspectos que se deben tener en cuenta en una investigación interna, desde los **principios** que deberían inspirar la actuación de las personas que la llevan a cabo (independencia, confidencialidad, profesionalidad – honradez (*truthfulness*), imparcialidad, legalidad – apartado 4.º de la guía) hasta las cuestiones básicas en materia de comunicación con **terceras partes interesadas** (*stakeholders*), incluidas las autoridades públicas (apartado 10.º).

Antes de establecer las fases y medidas que deberían integrar un procedimiento de investigación (apartado 8.º) se subraya la importancia de que los **máximos órganos de dirección** de la organización muestren su compromiso con los principios que deben inspirar estas indagaciones, destinando los recursos que sean necesarios para que su implicación pueda considerarse real y efectiva (*tone from the top*). El reverso de esta exigencia es que los máximos responsables de la organización sean razonablemente informados de la existencia y curso de las investigaciones que se lleven a cabo (apartado 5.º).

El compromiso de los máximos órganos de dirección con los principios previstos en el apartado 4.º debe traducirse en una **política de investigaciones internas** en la que se concreten tales principios. Debe determinarse qué personas o funciones serán las competentes para acordar y/o conducir una investigación dentro de la organización, con qué facultades, con qué límites y, en todo caso, con qué derechos pueden contar las personas investigadas. Debe requerirse también

[1] Para un seguimiento individualizado del estado de implementación de la Directiva UE 2019/1937 véase: https://www.whistleblowingmonitor.eu/country/

la documentación de los resultados de la investigación, así como su confidencialidad, entre otros extremos (apartado 6.º).

Se considera asimismo indispensable adoptar **medidas para la protección** tanto **de las evidencias** personales (testigos) como reales (fuentes de prueba materiales, como por ejemplo documentos físicos y/o digitales, etc.). Igualmente se debe estar atento a las necesidades de protección de cualquiera **de las personas intervinientes** en la investigación, especialmente frente a represalias (apartado 7.º).

En cuanto al **procedimiento de investigación** en sentido estricto destacan varias directrices. Primero se requiere que el equipo cuente con el debido **mandato** (apartado 8.1.º) y que la línea de reporte interno de la investigación hasta el máximo órgano de dirección de la entidad esté definida desde un inicio (8.2.º). Se exige que el **alcance** objetivo, subjetivo y geográfico de la investigación estén definidos (8.3.º), documentando cualquier modificación al respecto. En materia de **confidencialidad** se compele a solicitar por escrito o verbalmente máxima confidencialidad a los intervinientes, bajo la advertencia de las consecuencias legales de una eventual filtración (8.6.º). Respecto de las entrevistas se confirma la necesidad de **documentar** su contenido, recabando la conformidad del entrevistado con el acta o documento que se levante dejando constancia de la conversación (8.9.º). También se exige documentar los resultados de la investigación **(informe final)**, aunque cuando exista un litigio iniciado o de previsible iniciación se requiere solicitar asesoramiento legal sobre la confidencialidad de la documentación generada con la investigación (8.11.º).

Aunque no tiene por qué formar parte del encargo realizado a un equipo de investigación interna, la guía también contempla los pasos a seguir en el supuesto de que se solicite al equipo la propuesta de **medidas de reparación** o **mejora** de la organización interna a la vista de las infracciones detectadas. Al respecto destacan la necesidad de tener en cuenta el principio de proporcionalidad y la de realizar un seguimiento de las medidas propuestas. En el marco de estas medidas debe contemplarse, también, la revisión del sistema de *compliance* a fin de minimizar la reiteración de infracciones similares en el futuro (apartado 10.º).

Por el momento la observancia de los estándares contenidos en esta guía no permite optar a certificado alguno de la Organización Internacional de Estandarización.

Puede consultarse este mismo comentario, publicado en la página web de MOLINS, en el siguiente enlace: https://www.molins.eu/la-nueva-iso-37008-guia-para-las-investigaciones-internas/

B) Jurisprudencia

- **Asunto *SEC* v. *COVINGTON & BURLING, LLP* ante la U.S. District Court for the district of Columbia.**

En el ámbito jurisprudencial ha sido noticia la resolución de la U.S. District Court for the district of Columbia dictada el 24/7/2023 en el asunto **SEC v. COVINGTON & BURLING, LLP**.

En enero de este año la agencia reguladora de los mercados financieros solicitó al mencionado tribunal que ordenara a la firma de abogados COVINGTON & BURLING LL.P. que cumpliera con el

requerimiento efectuado por la SEC consistente en la aportación de la identidad de 298 clientes suyos, así como el contenido de algunas de las comunicaciones intercambiadas con ellos.

La firma se opuso alegando que ello vulneraría el derecho/deber al secreto de las comunicaciones mantenidas con sus clientes. Ochenta y tres (83) despachos de abogados de los EE.UU. firmaron un informe presentado ante el Tribunal en calidad de *amici curiae* respaldando al despacho requerido.

El Tribunal avaló la petición de la SEC de forma limitada. Para una lectura de la resolución véase: https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2023mc00002/250898/42/

2. Europa

A) Normativa

En el año 2023 destacan, en el plano europeo, el Reglamento y la Directiva de la UE sobre acceso transfronterizo a fuentes de prueba electrónicas:

- **Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023,** sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.

- **Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023,** por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales.

Para más información sobre el particular, véase el siguiente enlace: https://www.consilium.europa.eu/es/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/

B) Jurisprudencia

- **Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala, de 14 de febrero de 2023, caso *Halet* v. *Luxemburgo*.**
  Temática: el derecho a la libertad de expresión de los delatores (*whistleblowers*) frente a sus deberes de lealtad y confidencialidad hacia sus empleadores. Límites a la justificación de "*whistleblowing*".

– Hechos:

En esta sentencia la Gran Sala del Tribunal Europeo de Derechos Humanos resuelve la demanda interpuesta en mayo de 2018 por un ciudadano de nacionalidad francesa, el Sr. Raphaël Halet,

que había sido condenado por las autoridades judiciales del Gran Ducado de Luxemburgo por delitos de hurto, receptación, acceso ilegítimo a un sistema informático y revelación de un secreto profesional, por haber entregado a un periodista dieciséis documentos obtenidos de la empresa por la que trabajaba, la auditora PricewaterhouseCoopers (PwC, en adelante).

La documentación consistía en: i) las devoluciones fiscales recibidas por catorce empresas multinacionales, internacionalmente conocidas y clientas de la auditora, fruto de los acuerdos tributarios avanzados (*Advanced Tax Agreements*) alcanzados con la administración tributaria luxemburguesa; ii) una carta enviada por la auditora a una de estas empresas en relación con un borrador de devolución fiscal; iii) así como una carta enviada por dicha empresa a las autoridades tributarias luxemburguesas informando sobre la transformación de la compañía en un grupo empresarial.

El Sr. Halet entregó tales documentos a un periodista (el Sr. E. P.) a finales de 2012, después de que a mediados de ese año se emitiera un primer reportaje por televisión sobre los ventajosos acuerdos fiscales alcanzados por las autoridades tributarias de Luxemburgo con numerosas empresas multinacionales. En aquel programa se difundieron miles de documentos confidenciales que otro ex empleado de PwC (el Sr. A. D.) había revelado con anterioridad al mismo periodista, en vulneración de sus deberes de confidencialidad y lealtad con la auditora.

Los documentos facilitados por el Sr. Halet fueron utilizados en un segundo reportaje de televisión, junto a otra información obtenida de múltiples fuentes, emitido en junio de 2013. En noviembre de 2014 el Consorcio Internacional de Periodistas de Investigación (*International Consortium of Investigative Journalists*) publicó en su página web en torno a veintiocho mil (28.000) páginas relativas a acuerdos de fiscalidad alcanzados entre las autoridades luxemburguesas y los clientes de PwC. Estas revelaciones públicas son conocidas como el caso *Luxleaks*.

En diciembre de 2014 PwC y el Sr. Halet alcanzaron un acuerdo privado en el que la compañía reducía sus reclamaciones civiles contra él a la simbólica suma de un (1) euro, junto con la facultad de inscribir una hipoteca por valor de diez (10) millones de euros sobre los activos del empleado. Asimismo, se acordó el despido del Sr. Halet una vez terminada su baja médica, un año después.

A raíz de la denuncia interpuesta por PwC, las autoridades judiciales de Luxemburgo condenaron a los Sres. A. D. y Halet por varios delitos, entre ellos los de hurto, receptación y revelación de secreto profesional. Si bien las penas que en abstracto cabía imponerles ascendían hasta los cinco (5) años de prisión, en aplicación del art. 10 CEDH (derecho a la libertad de expresión) y la doctrina del TEDH en relación con la especial protección que cabe conferir a los *whistleblowers* (*vid*. STEDH en el asunto *Guja* v. *Moldavia* [Gran Sala], n.º de demanda 14277/04, 12/2/2008) la Corte de Apelación luxemburguesa rebajó la pena del Sr. A. D. hasta los seis (6) meses de prisión, sanción que fue suspendida, y al Sr. Halet le impuso una multa de 1.000,00 €.

La Corte de Apelaciones nacional no eximió de responsabilidad penal al Sr. Halet porque entendió que no había satisfecho todas las condiciones de aplicación de la especial protección conferida a través del art. 10 CEDH a los *whistleblowers*, de acuerdo con la doctrina del TEDH al respecto sentada en el caso *Guja* v. *Moldavia*. Concretamente, el tribunal de apelaciones consideró que la información revelada por el demandante, si bien podía considerarse “alarmante y escandalosa”, no aportaba nada nuevo que pudiera considerarse esencial o fundamental para

relanzar o contribuir al debate público, teniendo en cuenta que, un año antes, el Sr. A. D. había revelado miles de documentos similares.

En consecuencia, la Corte de Apelaciones luxemburguesa consideró que el daño causado a PwC con la revelación pública de los documentos, en vulneración del deber de secreto profesional que pesaba sobre el Sr. Halet, preponderaba respecto del interés general que pudiera haber en tener acceso a la información filtrada por el demandante.

El Tribunal de Casación de Luxemburgo confirmó la sentencia de la Corte de Apelación en relación con el Sr. Halet. En relación con el Sr. A. D., en cambio, casó la sentencia del tribunal de apelación y acordó su libre absolución en virtud del art. 10 CEDH y el régimen de especial protección reconocido a los *whistleblowers*.

La demanda del Sr. Halet contra Luxemburgo ante el TEDH fue resuelta en primera instancia por la Sección 3.ª del tribunal de Estrasburgo en fecha 11/5/2021. Con cinco votos a favor y dos en contra la Sala falló en contra del demandante, concluyendo que no se había vulnerado su derecho a la libertad de expresión previsto en el art. 10 CEDH. La Sección 3.ª hizo suyo el argumento de la Corte de Apelaciones luxemburguesa relativo a que la información comunicada por el Sr. Halet no era "esencial, nueva y desconocida con anterioridad" a su comunicación, por lo que, al igual que el tribunal nacional, entendió que el daño causado a PwC pesaba más que el interés general en la información.

Tras conocer el fallo el demandante solicitó la remisión de su demanda a la Gran Sala, que la admitió a trámite el 6/9/2021.

- Contexto normativo internacional:

En relación con el marco legal aplicable para la resolución del caso el Tribunal de Estrasburgo se hace eco de las fuentes normativas aparecidas en el plano internacional y europeo desde su sentencia de 2008 en el asunto *Guja* v. *Moldavia*.

En el plano internacional destaca el informe A/70/361 de 8 de septiembre de 2015, del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión dirigida a la protección de las fuentes de información y de los *whistleblowers*.

En el plano europeo, cita la Resolución 1729 (2010) de la Asamblea Parlamentaria del Consejo de Europa (CoE) sobre la protección de los *whistleblowers*, de 29/4/2010. Se menciona también la Recomendación CM/REc (2014)7 del Comité de Ministros del Consejo de Europa sobre la protección de los *whistleblowers*. Asimismo, se recoge la Resolución 2300 (2019) de la Asamblea Parlamentaria del CoE, sobre la "Mejora de la protección de los *whistleblowers* en toda Europa".

Naturalmente se da cuenta también de la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, sobre la protección de las personas que denuncian vulneraciones del Derecho de la Unión, aprobada el 23/10/2019.

- Principales argumentos de las partes:

En nombre del Sr. Halet se formulan varias peticiones de orden metodológico. En primer lugar se solicita al Tribunal que aclare con qué orden deben aplicarse los requisitos que integran la conocida como doctrina *Guja*. Asimismo, le pide al Tribunal que determine si el análisis de estos

criterios debe realizarse de forma aislada o mediante una valoración global. En tercer lugar el demandante cuestiona con múltiples argumentos la conveniencia de tener en cuenta los perjuicios financieros, reputacionales o del orden que sea causados al actor/es del sector privado afectados por la revelación de la información. Según el demandante, tan solo se deberían tener en cuenta aquellos daños consistentes en las sanciones profesionales impuestas a tales actores como consecuencia de la revelación y solo cuando tales reprimendas fueran desproporcionadas. En nombre del Sr. Halet se pide también que el Tribunal ofrezca una definición de *whistleblower*. En cuanto al caso concreto, se critica la decisión de la Sección 3.ª del TEDH, en la medida en que convalida la interpretación de los tribunales nacionales de Luxemburgo en relación con la introducción de un nuevo criterio cuya aplicación restringe significativamente el ámbito de protección conferido a los delatores. A saber, el requisito de que la información revelada sea "esencial, nueva y desconocida antes de la revelación".

Por su parte, el Gobierno de Luxemburgo defendió el criterio acabado de mencionar, alegando que no se trata de un requisito nuevo, sino que se encontraba inherente en el quinto juicio de la doctrina Guja: el relativo al interés público de la información. Por lo que se refiere a los perjuicios causados por la revelación a tener en cuenta en la ponderación, el Gobierno subraya la importancia de los intereses financieros y reputacionales de los actores privados afectados por la revelación, haciendo notar que también existen razones de interés general en la protección de tales intereses particulares. Así, por ejemplo, en garantizar que los ciudadanos confíen su información sensible a determinados profesionales, a fin de que estos puedan prestar servicios considerados fundamentales para el buen funcionamiento de la comunidad.

- Argumentos de los terceros intervinientes (*amicus curiae*):

Las terceras partes intervinientes en el procedimiento ante el TEDH, consistentes en organizaciones no gubernamentales dirigidas al asesoramiento y/o protección de los *whistleblowers* o de los periodistas, alertaron, en primer lugar, de que el nueva exigencia relativa a que la información sea "esencial, nueva y desconocida con anterioridad" a la revelación iba a tener un fuerte efecto desaliento en los potenciales delatores, además de abonar la inseguridad jurídica sobre las condiciones para conseguir el régimen de protección especial. En concreto, criticaron que, con el nuevo requisito, el juicio sobre el interés público de la información que hasta entonces se hacía desde una pespectiva *ex ante* pasaba a realizarse desde una perspectiva *ex post*, lo cual resulta, obviamente, mucho más restrictivo y desfavorable para los *whistleblowers*.

Se alegó también que en muchas ocasiones es necesario alzar la voz (revelar información confidencial) más de una vez para que las autoridades públicas reaccionen. Advierten que los cambios institucionales profundos y a largo plazo normalmente solo se consiguen dando la alerta a través de los medios de comunicación de masas.

- Doctrina general sobre el régimen de especial protección a los *whistleblowers*:

En primer lugar la Gran Sala recuerda su doctrina en materia de especial protección de los *whistleblowers*, sentada en la Sentencia del asunto *Guja* v. *Moldavia*, de 2008. Dicha doctrina se asienta en seis juicios o criterios de análisis:

i) La existencia de canales (internos) alternativos para la comunicación de la información.
En este sentido el Tribunal recuerda que el agotamiento de los canales internos debería ser siempre prioritario (nm. 113).

ii) El interés público en la información revelada.
iii) La veracidad de la información comunicada.
iv) El perjuicio causado al empleador.
v) La actuación de buena (o mala) fe del informante.
vi) La severidad de la sanción impuesta al *whistleblower*.

Si bien el Tribunal manifiesta expresamente su voluntad de no ofrecer una definición general y abstracta de *whistleblower*, concreta algunos criterios para delimitar el ámbito subjetivo de su doctrina al respecto, sin perjuicio de que no sean inmutables (nms. 112, 116, 117, 118, 119):

- El informante se supone que es la única persona o una de las pocas personas que conoce la información, por lo que es la mejor posicionada para actuar en favor del interés público.

- La existencia de un deber de reserva que pese sobre el informante es un elemento clave. Si la persona no se enfrenta a un dilema (revelar en favor del interés general *v*. cumplir con un deber de confidencialidad en interés de su principal) el régimen de especial protección no resulta aplicable (nms. 117, 118).

  Esto excluiría a los *extraneus*, como por ejemplo activistas que irrumpieran en las instalaciones de una empresa contaminante, p.e., o periodistas de investigación.

- La situación "*de facto*" es más importante que el estatus formal de trabajador por cuenta ajena (nm. 119).

- La doctrina está pensada para una relación laboral (desde una perspectiva material – *de facto*). Los elementos clave son la existencia de un **deber de lealtad** – confidencialidad, por un lado, y la posición de **vulnerabilidad económica** del informante respecto del principal (nm. 119).

– Precisión de los criterios *Guja* y su aplicación, teniendo en cuenta que los criterios *Guja* son del año 2008 y el contexto europeo e internacional sobre *whistleblowing* ha cambiado mucho (nm. 120):

  - Los canales usados para llevar a cabo la comunicación (nms. 121-123)

El Tribunal insiste en que los canales internos deben ser prioritarios. Antes de revelar externamente se debe agotar la vía interna (nm. 121). Cita resoluciones recientes (*Bathellier* v. *Francia*, n.º demanda 49001/07; *Stanciulescu* v. *Romania*, n.º 14621/06) donde no se ha considerado vulnerado el derecho a la libertad de expresión del informante porque éste no agotó o no hizo uso de los canales internos de comunicación existentes en la organización a la que pertenecía.

Ahora bien, para que el canal interno sea prioritario debe existir y funcionar correctamente (nm. 122). Asimismo, se admiten excepciones cuando hay un riesgo cierto de represalias o de ineficacia (se presume que será así, p.e., cuando la información afecta a aspectos fundamentales de la actividad del principal).

Con todo, de forma un tanto inconsistente, el Tribunal acaba abriendo la puerta a que el agotamiento de la vía interna no sea considerada una obligación para el informante, remitiéndose

al análisis de las circunstancias de cada caso concreto. El TEDH justifica su inconsistencia amparándose en la CM/REc (2014)7 del Comité de Ministros del Consejo de Europa, lo cual hace un flaco favor a la necesidad de seguridad jurídica que cualquier cuerpo normativo o doctrina jurisprudencial debería favorecer (nm. 123).

- La veracidad de la información (nms. 124-127)

De nuevo el Tribunal se ampara en la **Recommendation (2014)7** para subrayar que si *ex post* se demuestra que la información no era correcta, no se debe retirar la protección al *whistleblower*. No es exigible que los delatores tengan una imagen completa y exacta de lo sucedido. El juicio relevante debe adoptar la perspectiva *ex ante*. En la misma línea cita la **Resolución 1729 (2010) de la Asamblea Parlamentaria del Consejo de Europa.**

- La actuación de buena fe por parte del informante (nms. 128 a 130)

El Tribunal considera que la motivación que guía al informante es un criterio decisivo a la hora de valorar el caso y conferirle protección. Considera relevante descartar el ánimo de lucro o de perjudicar al principal por algún conflicto previo (nm. 128).

Exige también que no se actúe sobre la base de meros rumores o sin base probatoria. En tales casos el informante no habría actuado de buena fe.

- El interés público en la información comunicada (nms. 131-144)

Al respecto el Tribunal aporta algunos criterios, pero, de nuevo, se remite al análisis del caso concreto como cláusula de cierre (nm. 144).

Los hechos que se refieren a la actuación del Gobierno, instituciones o servicios públicos es claro que son de interés público (nms. 132-135).

En segundo lugar el Tribunal establece una graduación en función del contenido de la comunicación. El Tribunal considera que las comunicaciones sobre comportamientos ilegales ocupan el primer lugar en la escala de contenidos con interés público. El segundo lugar es para aquellas conductas que son reprobables éticamente. En tercer lugar están aquellas cuestiones que dan lugar a un debate público sobre si la concreta conducta representa un daño para el interés general o no (nm. 140). El tercer grupo de informaciones es nuevo en la doctrina del TEDH. No estaba previsto en los anteriores precedentes.

Según el Tribunal, los tres grupos de información son relevantes y pueden justificar una vulneración del deber de confidencialidad, pero en medidas diferentes.

Es interesante tener en cuenta que los cinco votos particulares se refieren a este punto. El juez KJOLBRO rechaza el tercer nivel, por entender que debería quedar fuera del ámbito de protección del art. 10 CEDH. Los otros cuatro votos particulares consideran que el segundo y tercer grupo de informaciones son muy difíciles de delimitar, introduciendo un elevado nivel de inseguridad jurídica.

Entre las certezas que ofrece el Tribunal en su sentencia están, en primer lugar, que las cuestiones que afectan al bienestar y a la vida de la comunidad tienen una relevancia mayor que las cuestiones que afecten a compañías privadas o a particulares, aunque también podrían ser

de interés general. En este sentido, la actuación y funcionamiento de las instituciones o servicios públicos normalmente serán considerados de interés general (concreción en función del sujeto afectado por la comunicación – nms. 142).

- El daño causado (nm. 145-148)

Si bien la mayor parte de los casos a partir de los cuales el Tribunal ha desarrollado su doctrina en materia de *whistleblowing* se refieren a funcionarios públicos que han hecho revelaciones que han afectado a una autoridad o institución pública, incluyendo empresas públicas, la doctrina del Tribunal contempla también la posibilidad de tener en cuenta los perjuicios económico-financieros y/o reputacionales causados a la empresa o al particular afectado por la comunicación de un *whistleblower*.

Aparte, se deben tener en cuenta los perjuicios causados a la comunidad, ya sea por la afectación a la economía de la comunidad derivada de la revelación, ya sea por la afectación a la confianza del público en determinadas instituciones.

El Tribunal concluye que debe realizarse un análisis global que tenga en cuenta todas estas dimensiones a la hora de ponderar los intereses en juego en el caso concreto.

- La gravedad de la sanción (nm. 149-154)

La naturaleza (laboral, civil, administrativa, penal) y la severidad de las consecuencias jurídicas negativas impuestas al informante por haber vulnerado sus deberes de confidencialidad debe tenerse en cuenta a la hora de evaluar si se ha restringido de forma desproporcionada su derecho a la libertad de expresión.

Al respecto el Tribunal recuerda que el despido es la sanción laboral más grave que cabe imponer en el ámbito laboral (nm. 149). Señala, asimismo, que una condena penal, independientemente de la medida de la pena, es la consecuencia jurídica más grave que puede imponer el Ordenamiento Jurídico, advirtiendo que, a veces, la mera imposición de una condena penal puede ser más relevante que el tipo o intensidad de la pena concreta impuesta (nm. 151).

– La aplicación de los criterios expuestos al caso concreto:

Antes de proceder al análisis del caso concreto sobre la base de los criterios anteriormente expuestos el Tribunal aclara que no es preceptivo seguir un orden concreto de análisis, sin que exista una jerarquía entre criterios (nm. 170). El Tribunal establece que los jueces y tribunales nacionales deben realizar una análisis global de todos los criterios, teniendo en cuenta su interdependencia.

  - Canal utilizado (nms. 171-172):

Si bien el demandante no agotó la vía interna, el Tribunal considera que esto no es óbice en el presente caso para conferirle la protección del art. 10 CEDH. La razón es que, cuando los hechos objeto de comunicación no se refieren a un comportamiento ilegal, como no lo eran los acuerdos fiscales tramitados por PwC para sus clientes en Luxemburgo, no tiene sentido que el informante alerte a su superior jerárquico. En estos casos no es realista esperar que el principal reaccione, por lo que el recurso a la revelación pública deviene el único canal idóneo.

Esta conclusión, extremadamente discutible, es ventilada por el Tribunal de forma muy expeditiva. Probablemente el hecho de que la Corte de apelaciones interna (de Luxemburgo) alcanzara la misma conclusión lo explica. El problema es que con este argumento se rebajan las exigencias en materia de subsidiariedad (agotamiento de los canales internos o institucionales) cuando, precisamente, la información pertenece al menor nivel de importancia en términos de interés público: hechos que no son ilícitos ni reprobables pero que son aptos para abrir un debate público sobre su lesividad para el interés general.

- La veracidad de la información divulgada (nm. 173)

En el caso concreto se considera un hecho incontrovertido que la información revelada era veraz. Así lo concluye también la Corte de Apelaciones luxemburguesa.

- La buena fe del informante (nm. 174)

Se considera también un hecho incontrovertido.

- Ponderación del interés público y los daños causados (nms.175-204)

    - El contexto de la comunicación

El Tribunal subraya que el contexto de la revelación puede jugar un papel crucial a la hora de valorar el interés público en la información. En el presente caso se dio la particularidad de que la información filtrada por el demandante se produjo tras una primera filtración mucho más importante tanto cualitativa como cuantitativamente por parte de otro empleado a un periodista. La revelación previa había sido la primera sobre el asunto y se había producido y emitido un programa de televisión sobre la base de tales documentos. La información filtrada por el demandante simplemente confirmó el trabajo previo del periodista y fue objeto de un segundo programa sobre el mismo asunto, emitido un año después del primero.

El Tribunal señala que el debate público no debe verse como algo petrificado, congelado en el tiempo, sino como un proceso en continua evolución. Por ello, el hecho de que la información revelada no sea nueva no debería ser un obstáculo para conferir la protección del art. 10 al informante (nm. 184). De este modo el Tribunal responde a una de las preguntas clave del caso, a saber, si la información debe ser nueva en el debate público para que el *whistleblower* merezca protección.

El Tribunal manifiesta expresamente que toma nota de la objeción planteada por las terceras partes intervinientes, que habían dicho que este (nuevo) requisito introducía mucha inseguridad jurídica para los informantes (nm. 183).

    - El interés público en la información

La información revelada hace referencia a las políticas y prácticas fiscales del Estado de Luxemburgo en relación con empresas multinacionales. La revelación sirvió para contribuir a un debate, iniciado con las revelaciones previas de otro empleado de PwC al periodista E. P., sobre la justicia de políticas tributarias como las de Luxemburgo a nivel Europeo e internacional, en la medida en que servían a las empresas multinacionales como vías de elusión de las cargas fiscales que les correspondería asumir en sus países de origen.

El Tribunal considera que no cabe la menor duda de que una información que contribuye a enriquecer un debate sobre la justicia de determinadas políticas y/o prácticas fiscales con trascendencia europea tiene interés público.

En el caso concreto, el Tribunal considera que la información revelada es de interés público porque se podía considerar ”alarmante y escandalosa”, tal y como reconoció la Corte de Apelaciones luxemburguesa, así como porque ofreció ejemplos concretos y reales de las implicaciones que determinadas políticas fiscales de determinados estados en relación con las empresas multinacionales podían tener en una escala europea.

- Los efectos perjudiciales

En contra de lo solicitado por el demandante, el Tribunal tiene en cuenta los perjuicios sufridos por la empresa empleadora del demandante. Tanto los de carácter financiero como los reputacionales. Asimismo, tiene en cuenta los daños reputacionales y de otros intereses causados a los clientes de la empleadora, esto es, las multinacionales a quienes la información revelada hacía referencia.

El Tribunal identifica además un perjuicio al interés público, consistente en la merma de la confianza de los ciudadanos en el secreto de sus comunicaciones a determinados profesionales cuyo secreto profesional se considera clave para que los ciudadanos y entidades acudan a sus servicios, lo cual es de interés general. La revelación del informante afecta a una cuestión de política pública.

- Resultado de la ponderación

Aunque el Tribunal identifica muchos y relevantes efectos negativos, lesivos, de la revelación, entre ellos los daños reputacionales a PwC, el daño al interés general en que se respeten las prohibiciones penales de robo y violación del deber de secreto profesional, considera que el interés público de la información prepondera sobre tales daños, dado que la información se refiere a un tema de indudable interés general, como lo son las políticas y prácticas tributarias de un determinado estado. El Tribunal le da importancia al hecho de que la información era de interés no solo a nivel nacional, sino también a nivel de todo un continente, como el europeo.

- La severidad de la sanción

El mero hecho de que se imponga una condena al informante se considera muy relevante, independientemente de la severidad de la pena impuesta (en este caso una pena de multa de 1.000,00 euros).

La mera imposición de un castigo por las autoridades judiciales de un país conlleva un efecto desaliento que, según el Tribunal, no cabe admitir teniendo en cuenta el rol fundamental que los *whistleblowers* desempeñan en las sociedades democráticas.

Por ello concluye que una condena penal resulta desproporcionada en el caso objeto de enjuiciamiento.

- Votos particulares:

El fallo se adopta con doce votos a favor y cinco en contra. Los cinco votos contrarios son los de los jueces que integraron la Sección 3.ª y votaron a favor del fallo adoptado en la primera instancia del TEDH. La principal crítica es que la mayoría, pese a tener en cuenta un notable número de efectos perjudiciales de la revelación, tanto de naturaleza privada-particular como general-pública, concluye que el interés público de una información que no era nueva ni fundamental para el debate público de referencia debe prevalecer frente a tales perjuicios, lo cual no pueden compartir. Destaca un argumento: según la propia graduación hecha por la mayoría sobre la importancia de una determinada información para el interés público, advierten que la información del caso concreto se debería subsumir en la tercera categoría, la más baja, relativa a información sobre hechos conformes con la legalidad y no manifiestamente reprobables, cuyo interés radica en que contribuyen a estimular el debate público sobre su carácter perjudicial para la comunidad (vid. nm. 140 y ss.).

- **Sentencia del Tribunal Europeo de Derechos Humanos, Sección 4.ª, de 13 de diciembre de 2022, caso *Florindo de Almedia Vasconcelos Gramaxo* v. *Portugal*.** *Temática*: monitorización de trabajadores mediante GPS y derecho a la intimidad.

El pasado 3 de abril devino firme la Sentencia de la Sección 4.ª del Tribunal Europeo de Derechos Humanos (TEDH, en adelante), de 13/12/2022, en la que por cuatro votos a favor y tres en contra se concluye que no hubo vulneración del derecho a la **vida privada (art. 8 CEDH)** de un médico empleado en una compañía farmacéutica al que se le instaló un sistema de GPS en el vehículo que la empresa había puesto a su disposición para realizar las visitas comerciales a los clientes.

Las **circunstancias fácticas** más relevantes que el Tribunal de Estrasburgo considera probadas son las siguientes:

i) en septiembre de 2011 la compañía instaló un sistema de GPS en el vehículo de empresa puesto a disposición del demandante;

ii) en octubre de este mismo año el recurrente interpone una queja ante la autoridad nacional competente en materia de protección de datos (la *Comissão Nacional de Protecção de Dados* – la CNPD, en adelante);

iii) en noviembre de 2011 la compañía farmacéutica informa a la CNPD de la instalación del sistema de geolocalización en los vehículos de empresa de sus empleados.

iv) en enero de 2012 el demandante acusa recibo por escrito de haber recibido una nota informativa interna en la que se le comunicaba la instalación del sistema de GPS en su vehículo; la información que dicho sistema suministraba a la empresa en relación con los posicionamientos y trayectos realizados por el trabajador; la finalidad de control y fiscalización de los gastos de kilometraje declarados por los trabajadores perseguida con la instalación de dicho sistema; así como la posibilidad de adoptar medidas disciplinarias en caso de discrepancia entre lo declarado por el trabajador y los datos aportados por el aparato.

v) en septiembre de 2013 la CNPD notificó al demandante la decisión de archivar su queja sin sanción contra la farmacéutica, sin que este recurriera posteriormente la resolución ante la jurisdicción administrativa interna.

vi) en abril de 2014 se instala un segundo aparato GPS en el vehículo del demandante, dado que el primero presenta anomalías en su funcionamiento. Tras una inspección del primer aparato, la empresa instaladora informa de que las anomalías responden a una intervención externa.

vii) en mayo de 2015 la empresa abre un expediente disciplinario contra el trabajador demandante. Se le entrega una carta de cargos en la que se le informa de que en virtud de la información recabada con el sistema de monitorización de su vehículo mediante GPS se ha concluido que, entre noviembre de 2013 y mayo de 2014: a) ha realizado un número de kilómetros inferior en horario laboral al que realmente declara, con la finalidad de disimular los kilómetros que realiza durante su tiempo libre (fines de semana y festivos); b) ha manipulado el aparato para evitar poder ser monitorizado por la empresa.

viii) tras un proceso interno de carácter contradictorio el trabajador es despedido en septiembre de 2015.

Aunque no conste en el apartado de hechos probados de la sentencia, de los razonamientos jurídicos se pueden considerar asimismo hechos incontestables los siguientes, que, a nuestro juicio, son también relevantes:

ix) el sistema de geolocalización instalado funcionó durante las veinticuatro (24) horas del día, los siete (7) días de la semana.

x) la empresa farmacéutica no obtuvo la autorización de la CNPD para usar el sistema de GPS instalado hasta la segunda mitad de 2015. La obtención de esta autorización con carácter previo al uso de estos sistemas era una exigencia legal en el momento de los hechos.

Tras fijar los hechos objeto de análisis el Tribunal declara que la actuación de la empresa farmacéutica constituyó, sin lugar a dudas, una **injerencia** en la vida privada del trabajador demandante. Según la Sala, los datos de geolocalización del vehículo de trabajo de un empleado por cuenta ajena son información que afecta a su esfera de privacidad, al igual que las imágenes de un trabajador (*López Ribalda* et al. v. *España* (Gran Sala), n.º 1874/13, de 17/10/2019), sus mensajes electrónicos (*Barbulescu* v. *Rumanía* (Gran Sala), n.º 61496/08, de 5/9/2017) o los ficheros informáticos guardados por éste en el disco duro de la computadora corporativa (*Libert* v. *Francia*, n.º 588/13, de 22/2/2018).

A partir de aquí el TEDH analiza la posible vulneración del derecho a la vida privada del trabajador demandante (art. 8 CEDH) desde la óptica de las obligaciones positivas del Estado, esto es, en el sentido de examinar si las autoridades portuguesas velaron lo suficiente por el derecho a la vida privada del demandante ante la injerencia llevada a cabo por un particular, en este caso el empresario empleador. En este sentido concluye, en primer lugar, que en el momento de los hechos existía en Portugal un marco legal lo suficientemente garantista, sin que el demandante lo haya puesto en duda.

Sentado lo anterior, la cuestión clave es si las autoridades judiciales portuguesas ponderaron correctamente los derechos en liza, a saber, el derecho a la vida privada del trabajador (art. 8 CEDH) y el derecho – deber de control del empresario. Sobre la base de los criterios de análisis establecidos por la Gran Sala en *Barbulescu* v. *Rumanía* y en *López Ribalda* v. *España*, que el

Tribunal recuerda en el § 109 de la sentencia, concluye que la ponderación ha sido adecuada y, por tanto, no vulneradora del Convenio. La Sala fundamenta su decisión en tres razones:

i) el trabajador fue **debidamente informado** con carácter previo a la instalación del GPS en su vehículo de trabajo, además de habérsele comunicado la información que se iba obtener con dicho sistema de geolocalización, el uso que se haría de la misma, así como la posibilidad de recurrir a medidas disciplinarias sobre la base de tales datos.

ii) las autoridades judiciales portuguesas inadmitieron como fuente de prueba buena parte de los datos obtenidos por el sistema de GPS, valorando únicamente aquellos estrictamente **necesarios** para el control del kilometraje del trabajador. Dicho control resulta difícil de llevar a cabo sin recurrir al sistema de geolocalización.

iii) los datos obtenidos por el sistema de GPS han sido accesibles a un número muy reducido de personas, por lo que la injerencia ha tenido un **impacto limitado** en la vida privada del demandante.

Como se ha dicho, la sentencia cuenta con el voto particular de tres de los siete integrantes de la sección, de manera que la resolución fue aprobada por la mínima. Además, los magistrados disidentes discrepan de las razones de fondo en las que descansa el fallo. A su juicio el Tribunal debería haber estimado la demanda, declarando vulnerado el derecho a la vida privada del recurrente. Por tres razones. Primero, porque la monitorización fue especialmente invasiva, en la medida en que se prolongó durante más de dos años, controlando la posición del vehículo durante las **veinticuatro (24) horas del día, los siete (7) días de la semana**. Esto incluye, como es obvio, el tiempo libre del trabajador, lo que según la propia doctrina del TEDH es una afectación muy seria de su derecho a la vida privada. Segundo porque la actuación de la empresa durante el tiempo de la monitorización objeto de enjuiciamiento **no contó con la cobertura legal** requerida, a saber, la autorización de la CNPD. Tercero, porque **existía una medida menos invasiva** para conseguir el mismo objetivo de supervisión: instalar un interruptor que permitiera delimitar las horas de jornada laboral respecto de las horas de tiempo libre, dejando fuera del control este segundo ámbito de la vida del trabajador.

- **Sentencia del Tribunal de Justicia de la Unión Europea, Sala 5.ª, de 26 de enero de 2023, asunto C-205/21.**
  Temática: (dis)conformidad con el Derecho de la Unión de la recogida sistemática de los datos biométricos de una persona investigada por las autoridades públicas, con fines de prevención delincuencial.

En esta resolución el máximo intérprete del Derecho de la Unión resuelve la solicitud de decisión prejudicial formulada por un juzgado del orden penal búlgaro en relación con la normativa aplicable en su país en materia de registro de datos biométricos por parte de las autoridades policiales en la fase de investigación de delitos públicos de carácter doloso.

De acuerdo con la Ley del Ministerio del Interior vigente en el momento de los hechos en Bulgaria (*zakon sa Ministerstvo na vatreshnite raboti* – ZMVR, en adelante) las autoridades policiales debían incluir en un registro policial a las personas investigadas por delitos públicos dolosos (art. 68.1 ZMVR). A los efectos del registro, las autoridades policiales debían incluir una fotografía del investigado, sus huellas dactilares y una muestra de ADN (art. 68.3 ZMVR). En el caso de que

la persona investigada se negara a colaborar, los datos mencionados se debían obtener por la fuerza previa autorización judicial (art. 68.5 ZMVR).

Entre las varias cuestiones planteadas por el órgano judicial búlgaro al Tribunal de Justicia de la Unión Europea destaca la que pregunta por la compatibilidad de los preceptos anteriormente citados con la **Directiva (UE) 2916/680**, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Concretamente, la pregunta versaba, literalmente, como sigue:

> - ¿Es compatible con los artículos 10, 4, apartado 1, letras a) y c), y 8, apartados 1 y 2, de la Directiva 2016/680 una ley nacional —artículo 68, apartados 1 a 3, de la [ZMVR]— que establece como regla general la realización de fotografías de identificación, la toma de huellas dactilares y la obtención de muestras para la elaboración de un perfil de ADN de todas las personas investigadas por un delito público doloso?»

La respuesta del TJUE en la sentencia comentada es negativa: la Ley del Ministerio del Interior búlgara vigente en el momento de los hechos es incompatible con el Derecho de la Unión, concretamente con las exigencias previstas en el art. 10 de la Directiva 2016/680 en relación con los arts. 4.1.a)-c) y 8.1 y .2 de la misma norma, en las que se establecen y concretan los **principios de limitación de los fines** perseguidos con el tratamiento de los datos y el **principio de minimización** de los datos tratados.

Partiendo del carácter sensible de los datos biométricos, el Tribunal de Luxemburgo recuerda la importancia de respetar el **principio de subsidiariedad** a la hora de adoptar medidas que comprometan la privacidad del ciudadano, agotando cualquier medio alternativo menos invasivo que permita alcanzar el objetivo perseguido con la medida en cuestión. En este sentido señala que el registro de otra categoría (tipo) de datos podría cumplir igualmente la finalidad perseguida. Así, por ejemplo, los datos de estado civil (§§ 126, 133).

En segundo lugar, el Tribunal advierte que el requisito establecido por el art. 10 en el sentido de que la recogida y tratamiento de datos sensibles (como los biométricos o los relativos al ADN) sea **"estrictamente necesario"** obliga a que dicha recogida y tratamiento respondan a una finalidad muy concreta. Al respecto, el Tribunal declara que «*el mero hecho de que se investigue a una persona por la comisión de un delito público doloso no puede considerarse un dato que permita presumir, por sí solo, que la recogida de sus datos biométricos y genéticos es estrictamente necesaria a la vista de los fines que persigue y habida cuenta de las vulneraciones de los derechos fundamentales, en particular, de los derechos al respeto de la vida privada y de protección de los datos personales garantizados por los artículos 7 y 8 de la Carta, que de ella se derivan*» (§ 130).

En efecto, tal y como advierte el Tribunal, pueden «*darse casos en los que la recogida tanto de los datos biométricos como de datos genéticos no obedezca a ninguna necesidad concreta a efectos del procedimiento penal en curso*» (§ 131). Al respecto el Tribunal señala que el hecho de que la persona se encuentre investigada significa que ya existen suficientes elementos de prueba de su implicación en la infracción, por lo que la obtención de sus datos biométricos o genéticos no sería necesaria como medida adoptada de forma sistemática o por defecto (§ 131). Entendemos que otra cuestión sería que la obtención de estos datos sirviera para determinar el sentido (incriminatorio o de descargo) de una concreta fuente de prueba.

A fin de acotar el ámbito de aplicación de la Directiva y, por tanto, los casos en los que sí se podría considerar justificada la recogida y tratamiento de datos sensibles como los biométricos o los de ADN el Tribunal señala, a título meramente ejemplificativo, alguno de los criterios que habría que tener en cuenta a la hora de decidir si tal recogida es crucial para la prevención o persecución de otros hechos delictivos, distintos a los que son objeto del procedimiento en el marco del cual se obtienen los datos biométricos o genéticos. Según el tribunal, a tal efecto debería tenerse en cuenta: i) la naturaleza y gravedad de la presunta infracción por la que la persona se encuentra investigada; ii) las circunstancias concretas de esta infracción; iii) el eventual vínculo de dicha infracción con otros procedimientos en curso; iv) los antecedentes judiciales o el perfil individual de la persona en cuestión.

4. España

A) Normativa

La aprobación y entrada en vigor de la **Ley n.º 2/2023**, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, es sin lugar a dudas el principal hito normativo del año a nivel interno.

Junto a él cabe añadir la publicación de la **Guía sobre Tratamientos de Control de Presencia Mediante Sistemas Biométricos**, de la Agencia Española de Protección de Datos.

- **Ley n.º 2/2023, de 20 de febrero, de protección de los informantes.**

Con esta nueva norma se cumple —con más de un año de retraso— la obligación de trasponer la Directiva (UE) n.º 2019/1937, de 23 de octubre, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Empleando terminología inglesa también se conoce como **Directiva *Whistleblowing***.

Esta ley obliga tanto a las entidades del sector privado como a las del sector público a dotarse de un **sistema interno de información** a través del cual cualquier integrante de la organización pueda comunicar, a través de un canal interno de denuncias, las infracciones que constituyen el ámbito objetivo de la norma.

El legislador concreta las características que debe reunir dicho sistema, entre ellas disponer de mecanismos que permitan recabar denuncias tanto por escrito como verbalmente, nominativas o **anónimas** (art. 7.3); estar dotados de medidas que preserven la confidencialidad de todo el procedimiento y, en particular, la identidad del denunciante; contar con un responsable del sistema designado directamente por el órgano de administración o de gobierno (persona que en el sector privado debe tener la condición de **directivo** – art. 8.5); disponer de una política sobre los principios que guíen el funcionamiento del sistema, que, junto al aplicativo para denunciar, debe publicarse de forma intuitiva y visible en la **página web** de la entidad, en caso de existir (art. 25); contar con medidas de protección específicas de los informantes frente a represalias; etcétera (*vid*. arts. 5 a 8).

Se regula también el procedimiento de comunicación con el denunciante, imponiéndose el deber de acusar recibo de la comunicación en un plazo máximo de siete (7) días naturales. Sin

embargo, excepto en relación con algunas cuestiones puntuales, no se establecen normas de procedimiento que regulen de forma completa la eventual **investigación interna** que decida llevar a cabo la correspondiente entidad pública o privada. Ello a pesar de que el legislador parte de la premisa de que tales investigaciones se pueden (¡o deben!) llevar a cabo. Así, por ejemplo, se fija un plazo máximo de tres (3) meses para "*dar respuesta a las actuaciones de investigación*" desplegadas (art. 9.2.d)). También se impone el deber de llevar un libro-registro respecto de las comunicaciones recibidas o de las investigaciones internas conducidas: «[t]*odos los sujetos obligados (…) deberán contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar*…» (art. 26.1; subrayado añadido).

Todo esto sin perjuicio del deber de informar al **Ministerio Fiscal** «*con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito*» (art. 9.2.j)). Esta previsión deberá interpretarse de modo que sea compatible con el derecho a no autoincriminarse de la persona jurídica, previsto en el art. 409 bis LECrim.

El único procedimiento de investigación que se regula expresamente de forma completa es el que vaya a seguir la **Autoridad Independiente de Protección del Informante** que esté llamada a actuar (arts. 16 a 24). A nivel estatal este organismo público está aún por constituir. En el plano autonómico algunas comunidades ya han designado la entidad encargada de asumir las competencias asignadas a esta figura. En Cataluña, por ejemplo, corresponde ejercerlas a la Oficina Antifrau de Catalunya.

Las **infracciones** respecto de las que resulta aplicable el régimen jurídico previsto en la nueva ley son las que siguen: a) cualquier infracción penal; b) cualquier infracción administrativa grave o muy grave; c) las infracciones del Derecho de la Unión Europea previstas en el anexo de la Directiva n.º 2019/1937 (blanqueo de capitales, financiación del terrorismo, contratación pública, seguridad de los productos, seguridad del transporte, medio ambiente, salud pública, protección de consumidores, privacidad y protección de datos, etc.), las que afecten a los intereses financieros de la Unión o las que incidan en el mercado interior (*vid*. art. 2 de la Ley y el anexo a la Directiva)

Beneficiario de la protección legal es **cualquier empleado** que, directa o indirectamente (se incluyen a los de las empresas subcontratadas, por ejemplo), trabaje o haya trabajado por la correspondiente entidad pública o privada. Entre otros se incluye a los becarios, voluntarios, personas en proceso de selección y autónomos. También a los accionistas, partícipes y miembros del órgano de administración (*vid*. art. 3).

Destacan las obligaciones previstas en materia de **protección de datos** (arts. 29-34). La identidad del informante debe mantenerse bajo reserva mediante la adopción de medidas técnicas y organizativas adecuadas para conseguir tal objetivo. Las únicas excepciones a esta regla son las comunicaciones a la Autoridad judicial, el Ministerio Fiscal o a la Autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora (art. 33.3). En estos casos se deberá comunicar al informante la decisión de comunicar sus datos. Esta comunicación deberá ser previa a la revelación y debidamente motivada.

Se prevén asimismo medidas de **protección del informante frente a represalias** (arts. 35 a 41). Las medidas calificables de represalia se declaran prohibidas. A tal efecto se considera represalia, por ejemplo, cualquier medida laboral que, por acción u omisión, suponga un empeoramiento en la posición del informante: despido, degradación de categoría, terminación anticipada del contrato temporal tras superar el periodo de prueba o incluso la no conversión del

contrato temporal en uno de indefinido (art. 36.3.a)). Por regla general la protección tendrá una duración de dos años, que excepcionalmente podrá prorrogarse (art. 36.4). En los procesos judiciales o jurídico-administrativos se presumirá que los perjuicios sufridos por el informante (un despido, por ejemplo) constituyen una represalia si el informante demuestra «r*azonablemente*» que ha realizado una comunicación conforme a lo previsto en la misma ley (art. 38.4).

En materia de **sanciones** conviene advertir que se prevén multas pecuniarias de un importe significativo, tanto para las personas jurídicas como para las personas físicas responsables del sistema interno de información, entre otros potenciales infractores (también pueden incurrir en responsabilidades los informantes desleales u otras personas que intervengan en el procedimiento iniciado tras la presentación de la comunicación). Las sanciones a las personas físicas oscilan entre los mil y un (1.001) y los trescientos mil (300.000) euros. Las previstas para las personas jurídicas ascienden hasta el millón (1.000.000) de euros (arts. 60 a 67).

Las infracciones **prescriben** a los tres años las muy graves, a los dos años las graves y a los seis meses las leves (art. 64). Los mismos plazos rigen para la prescripción de las sanciones.

Se incluyen **medidas de clemencia** que llegan hasta la exención de responsabilidad para quienes colaboren con las autoridades satisfaciendo determinadas condiciones (art. 40).

Para un análisis crítico de la norma véase el comentario redactado por el consultor de nuestra firma, el **Prof. Dr. Ramon Ragués i Vallès**, catedrático de Derecho penal en la Universitat Pompeu Fabra, publicado en la revista **La Ley Compliance Penal, n.º 13 del 2023**, bajo el título: "La Ley 2/2023 de protección de informantes: una primera valoración crítica".

- **Guía sobre Tratamientos de Control de Presencia Mediante Sistemas Biométricos**

En el mes de noviembre de 2023 la Agencia Española de Protección de Datos publicó la Guía sobre Tratamientos de Control de Presencia Mediante Sistemas Biométricos (31 páginas).

La Agencia adopta una postura muy restrictiva respecto del uso de los sistemas de identificación de personas físicas o autenticación biométricos para el control de presencia, en particular en el ámbito laboral, pero también en relación con otros ámbitos.

La autoridad española en materia de protección de datos considera que, por regla general, no será lícito el uso de este tipo de tecnologías para el registro de la jornada laboral o el control de acceso a determinados espacios. La razón es, básicamente, que existen otros medios de control menos invasivos e igual de eficaces para la finalidad perseguida, por lo que el recurso a las tecnologías basadas en el tratamiento de datos biométricos no sería, en principio, necesario. Como recuerda la Agencia, durante siglos se han realizado controles de la jornada laboral a través de diversos métodos ajenos al tratamiento de datos biométricos (exhibición de documentos, tarjetas identificativas, uso de códigos o claves, etc.), sin que consten deficiencias insalvables que los hiciera inútiles. Además, por lo menos desde 1890 han existido sistemas automatizados de control de jornada sin necesidad de recurrir a datos biométricos.

El estricto test de necesidad aplicado por la Agencia se basa en la consideración que el tratamiento de datos biométricos, en concreto con la finalidad de realizar un control de presencia, constituye un tratamiento de datos personales de categorías especiales. En este sentido la autoridad española reconoce haber cambiado su postura respecto de la guía publicada en mayo

de 2021 bajo el título “La Protección de Datos en las Relaciones Laborales”, donde se establecía que la autenticación biométrica en el marco de los tratamientos de registro de presencia no constituía un tratamiento de categorías especiales de datos. Según la Agencia, esta postura se ha visto superada por las Directrices 5/2022 del Comité Europeo de Protección de Datos (CEPD).

El rigor de la AEPD llega hasta el punto de descartar el consentimiento del empleado como excepción válida para levantar la prohibición de tratamiento. En este punto la argumentación de la autoridad resulta un tanto confusa, puesto que por un lado sostiene que el motivo de rechazar el consentimiento del trabajador como fuente de legitimación serían las dudas sobre la verdadera voluntad del empleado, en la medida en que la relación entre él y el empresario es asimétrica en términos de poder de negociación, por lo que resulta razonable cuestionar la veracidad del eventual consentimiento prestado por el trabajador en este ámbito.

No obstante, la Agencia rechaza también el uso de los sistemas de identificación/autenticación biométricos cuando media consentimiento del trabajador y, además, la posibilidad de elegir libremente entre dicho sistema y otro de alternativo con el que no se recogieran datos biométricos. En este caso la razón por la que se rechazaría la legitimidad del uso del sistema sería la evidente falta de necesidad de recurrir a este tipo de sistemas, en la medida en que sería obvio que existirían medios alternativos menos invasivos. Es cierto que no habría necesidad, pero se impediría al trabajador aprovecharse libremente de las ventajas que le pueda ofrecer, a su juicio, el sistema. La postura de la AEPD es significativamente paternalista.

Para un análisis en profundidad de la cuestión, véanse las consideraciones de la Agencia contenidas en la mencionada guía, consultable en el siguiente enlace:
https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

B) Jurisprudencia

- **Sentencia del Tribunal Constitucional n.º 92/2023, Sala segunda, de 11 de septiembre.**
  Temática: Límites a la video-vigilancia policial como fuente de prueba válida.

El pasado 11 de septiembre de 2023 el Tribunal Constitucional dictó la Sentencia n.º 92/2023. En esta resolución se resuelve una demanda de amparo que según la Sala presenta una especial trascendencia constitucional en relación con el derecho fundamental a la intimidad (art. 18 CE): la validez de las imágenes obtenidas por la Policía en un garaje de una comunidad de vecinos a través de la instalación de cámaras de grabación de imágenes, sin el preceptivo permiso de la comunidad de propietarios y sin autorización judicial para ello.

En el supuesto analizado, el Juzgado de lo Penal núm. 4 de Barcelona condenó a dos personas como autores de un delito de tráfico de drogas en su modalidad de sustancias que no causan un grave daño a la salud a la pena de tres años y un día de prisión y multa de seiscientos mil euros. La defensa de los condenados alegó que se produjo una vulneración de su derecho a la intimidad personal ya que la Policía instaló dichos dispositivos de grabación de imágenes en el garaje comunitario donde se encontraba estacionado el vehículo de uno de los acusados y dónde se encontraron 44 kilos de hachís cuando se procedió a su registro. Entiende el Juzgado de lo Penal n.º 4 de Barcelona que “*los garajes no tienen la consideración de domicilio constitucionalmente protegido, por lo que las grabaciones videográficas obtenidas en dichos espacios no requieren*

de autorización judicial y tienen validez como prueba de cargo para desvirtuar la presunción de inocencia".

Para seguir leyendo consúltese el comentario completo en: https://www.molins.eu/limites-a-la-video-vigilancia-policial-como-fuente-de-prueba-valida-comentario-a-la-stc-n-o-92-2023/

- **Sentencia de la Sala de lo penal del Tribunal Supremo n.º 436/2023, de 7 de junio, p. Berdugo Gómez de la Torre.**
  Temática: efecto reflejo de la declaración de ilegalidad respecto de un registro informático.

En su Sentencia n.º 436/2023 la Sala segunda del Tribunal Supremo resuelve el motivo planteado por un recurrente en casación que denuncia la vulneración de varios derechos fundamentales, entre ellos el derecho a la intimidad (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE). Aduce el justiciable que el Tribunal de instancia valoró prueba derivada de un registro ilegítimo de su cuenta de correo electrónico corporativa.

Los hechos que aquí interesan consisten en que la firma Deloitte analizó la cuenta de correo electrónico corporativa de varios empleados de la Caja de Ahorros del Mediterráneo (CAM), incluido el recurrente, por encargo de los administradores provisionales de la entidad financiera. El registro se llevó a cabo a pesar de que ninguno de los trabajadores había prestado su consentimiento y de que en ningún momento de la relación laboral se les había advertido de que un registro de tales características podía tener lugar.

La auditora elaboró un informe en el que se sacaban conclusiones fácticas sobre el caso objeto de enjuiciamiento. Según el recurrente, tales conclusiones formaban parte fundamental del informe y se basaron en los correos analizados sin cobertura legal.

El Tribunal a quo dio parcialmente la razón al recurrente y consideró prueba ilícita los correos electrónicos objeto del informe de Deloitte, así como otras derivadas directamente de tales mensajes. No obstante, confirió validez a las partes del informe que consideró desconectadas de los correos, así como a las demás pruebas que, a su juicio, no guardan conexión directa con los mensajes intervenidos.

Para seguir leyendo véase el comentario completo en: https://www.molins.eu/el-descafeinado-efecto-reflejo-de-un-registro-informatico-ilegitimo/

- **Sentencia de la Sala de lo penal del Tribunal Supremo n.º 89/2023, de 10 de febrero, p. Puente Segura (caso Pescanova).**
  Temática: doctrina general sobre el régimen jurídico aplicable en las investigaciones internas. En especial, sobre las condiciones de admisibilidad de la prueba obtenida mediante un registro informático.

En el Fundamento Jurídico Trigésimo de la STS (Sala Segunda) n.º 89/2023, caso Pescanova, el Tribunal examina el motivo planteado por uno de los recurrentes, consistente en objetar la admisibilidad como fuente de prueba de los correos electrónicos obtenidos en la indagación efectuada por KPMG a instancias del Consejo de Administración de PESCANOVA (27/2/2013), encargo posteriormente convalidado por la administración concursal (28/4/2013).

El recurrente alegó que, si bien el día 28/5/2013 otorgó su consentimiento al equipo de KPMG para que analizara los mensajes que había enviado y recibido a través de su cuenta de correo electrónico corporativa, nadie le informó de que los resultados del informe de la auditora estaban destinados a incorporarse al procedimiento penal (Diligencias Previas nº 31/2013) seguido ante el Juzgado de Instrucción nº 5 de la Audiencia Nacional, a petición del propio Juez instructor. En efecto, cinco días antes de que el recurrente prestara su consentimiento, el 23/5/2013, el Juez dictó Auto acordando solicitar a KPMG la remisión de su informe forensic. El día en el que el recurrente prestó su consentimiento al registro informático no ostentaba la condición de investigado en el procedimiento penal seguido ante el Juzgado Central de Instrucción nº 5. Los correos electrónicos encontrados por la auditora fueron medios de prueba decisivos para fundamentar el procesamiento penal y la posterior condena del recurrente.

En el Fundamento Jurídico Cuadragésimo Segundo se examina el motivo planteado por otro recurrente en el mismo sentido que el anterior, pero con una diferencia notable: en este caso el condenado no había prestado su consentimiento a KPMG para que analizara su cuenta de correo corporativo, lo que no fue impedimento para que la auditora inspeccionara sus mensajes y estos fueran posteriormente incorporados al procedimiento penal.

Para seguir leyendo véase el comentario completo en: https://indret.com/revista-critica-de-jurisprudencia-penal-el-caso-pescanova-2/

- **Sentencia de la Sala de lo contencioso-administrativo del Tribunal Supremo n.º 1207/2023, de 29 de septiembre, p. Navarro Sanchís.**
  Temática: condiciones de acceso de la AEAT a datos contenidos en dispositivos electrónicos.

El pasado 29 de septiembre de 2023, la Sección 2ª Sala de lo Contencioso Administrativo del Tribunal Supremo (en adelante, TS) fijó algunas de las condiciones de acceso por parte de la Agencia Española de la Administración Tributaria (en adelante, AEAT) a datos contenidos en dispositivos electrónicos (ordenadores, teléfonos móviles, tabletas, memorias, discos duros, entre otros) y detallado en qué supuestos se entienden infringidos los derechos fundamentales al secreto de las comunicaciones, y a la intimidad personal y familiar del artículo 18 de la Constitución Española.

Veamos las circunstancias concretas del caso. La Dependencia de Inspección de la Delegación Especial de la AEAT de Murcia inició un procedimiento de inspección a una persona física representante de distintas sociedades (Don J.M), a fin de garantizar el cumplimiento de pago de algunos tributos. Los inspectores, en el curso de la inspección y tras considerar que la información proporcionada por el ahora recurrente era incompleta, solicitaron al mismo que les permitiera realizar una copia del ordenador portátil con el que venía trabajando con habitualidad a fin de inspeccionar información con trascendencia tributaria contenida en el dispositivo. Siendo que el afectado se negó, los actuarios procedieron a adoptar como medida cautelar -sin contar con autorización judicial alguna- la copia y precinto en un disco duro de la información del equipo portátil a fin de proceder a su apertura tras obtener autorización judicial.

No fue hasta cinco meses más tarde cuando se aprobó la autorización judicial de acceso y copia de los mentados datos obrantes en el disco duro precintado, por parte del Juzgado de lo Cont. Admin. núm. 5 de Murcia.

Resulta interesante recalcar que ya en el Auto que se autorizaba a la copia y precinto del disco duro, confirmado por el TSJ de Murcia, se indicaba que el "lugar" digital es asimilable al hogar o domicilio personal y estamos ante la "garantía de intimidad informática", motivo por el que se hace más que evidente que era exigible autorización judicial para acceder al contenido de un dispositivo corporativo.

Contra el mentado Auto de autorización de entrada, Don J.M interpuso recurso de apelación ante la Sección 2ª de la Sala de lo Cont. Admin. del TSJ de Murcia, el cual fue desestimado en primera instancia por entender que la medida cautelar estaba justificada en base al triple juicio de idoneidad, necesidad y proporcionalidad, y cumplimentado con el principio de subsidiariedad.

Con posterioridad, la Sentencia dictada por la Sección 2ª de la de la Sala de lo Cont. Admin. del TSJ de Murcia fue recurrida por parte de Don J.M en casación ante la Sala 3ª Sección 2ª del TS, recurso el cual fue estimado por el Alto Tribunal y objeto de análisis por medio del presente.
Como consideración inicial, el propio TS hace referencia a la ausencia de expediente administrativo relativo a la inspección. Alude que no constaba ninguna actuación o documento de la AEAT atinente al proceso de inspección que se llevó a cabo, así como a la incautación del ordenador personal del contribuyente, hecho que les provocaba, literalmente "en cierto modo, a decidir a ciegas".

Por un lado, indica que la mera captación de datos exige autorización judicial, más aún el acto de copiado de datos y precinto. Este, debe ser motivado y plasmado en una resolución, garantizando que el precinto impide el examen del contenido del dispositivo, indicando de forma detallada cómo se almacena en la nube… y notificado al titular del aparato objeto de la medida.
Por otro lado, considera que los derechos fundamentales que podrían estar en juego en la adopción de esa medida cautelar son el derecho a la intimidad personal y familiar y el derecho al secreto de las comunicaciones, pero en ningún caso se trata del derecho a la inviolabilidad del domicilio (art. 18.1 CE) por considerar que no merecen el máximo nivel de protección constitucional. Asimismo, alude al nuevo derecho fundamental de última generación denominado "derecho al entorno visual", el cual recibe un tratamiento asimilable a los derechos anteriormente referenciados.

A mayor abundamiento considera que se requiere de autorización judicial al copiado cuando se afecte al derecho al secreto de las comunicaciones, empero no será necesaria cuando se afecte al derecho a la intimidad, siempre que se respete los principios de proporcionalidad, urgencia y necesidad.

Establece que el deber de proporcionalidad requiere separar antes del copiado los datos con trascendencia fiscal de los que no lo tengan, pues solo los primeros podrán ser examinados por la Inspección Tributaria.

Con todo, no constaban requerimientos incumplidos por parte del investigado, así como tampoco documentación ocultada o presentada de forma incompleta o tardía a la Administración. Considera que la supuesta "escasa colaboración y solo abstractamente insinuada" debería de haber sido detallada, así la falta de colaboración hubiera derivado a un proceso administrativo sancionador por infracción del art. 203 LGT (resistencia, obstrucción, excusa o negativa a las actuaciones de la Administración).

No cabe extender los requisitos jurisprudenciales exigidos para la autorización de entrada en domicilio a supuestos que no constituyan efectivamente una "entrada", como podría ser la

captación de datos o intervención de dispositivos en el curso de una entrada en domicilio. Solo sería posible mediante una reforma legal, de lo contrario, se generaría inseguridad jurídica.

Asimismo, estima el Alto Tribunal que no hubo acta o documento administrativo que acreditara el precintado y por ello, no se garantizó la imposibilidad material de acceso al contenido del dispositivo. Cabría una sospecha que, más allá de la copia del dispositivo, la AEAT tuvo posibilidad de examinar su contenido. Más aún cuando la Administración tardó más de tres meses desde la incautación y la solicitud de "entrada. Así, lo considera un "sacrificio desproporcionado e injustificado de derechos fundamentales" y reflexiona en favor de la posible aplicación subsidiaria del artículo 588 sexies de la LECrim y siguientes, sin olvidar los principios rectores del artículo 788 bis a) del mismo cuerpo legal, sobre los cuales trata la Circular 1/2019 de la Fiscalía General del Estado.

Por último, manifiesta que el consentimiento para el copiado aceptado por el investigado podría entenderse prestado bajo coacción o una aceptación forzada: "Ante su negativa a facilitar su ordenador portátil, se le advierte de que le sería incautado, sin posible tercera opción. Así, considera literalmente que el copiado era el mal menor que le esperaba". Consecuencia de ello, sopesa la medida cautelar adoptada como un exceso derivado de la negativa del contribuyente a colaborar. Y es que el mero copiado, aun con precinto, ya se considera invasor de derechos fundamentales.

A mayor abundamiento, afirma que el ordenador es un lugar que puede considerarse domicilio y que, siendo que en el presente supuesto no se prestó consentimiento no ya a la entrada, sino a la entrega o precinto del ordenador, se debió de haber contado con previa autorización judicial. Además, considera que el estado donde sucedieron los hechos, desde el año 2018 no es considerado jurisdicción no cooperativa ni mucho menos paraíso fiscal (St. Kitts & Nevis). De serlo, podría haberse acreditado la imposibilidad de solicitar y obtener la información tributaria relevante, empero no es el caso.

Por todo ello, concluye que el contribuyente tenía pleno derecho a negarse a prestar consentimiento en la entrada –negarse a entregar su ordenador personal- por afectar a su esfera de intimidad personal y al secreto de las comunicaciones, y ello, no puede servir como una "especie de castigo" en forma de medida cautelar, salvo supuestos de resistencia, excusa u obstrucción ante la inspección.

Además, cuando un Juzgado de lo Cont. Admin. autoriza el acceso a una información constitucionalmente protegida, se exige, i) justificar la necesidad de precintar y/o copiar datos a priori, ii) un control a posteriori de la actuación llevada a cabo por la Inspección, precisando en todo caso en qué consiste ese control, el límite temporal del mismo y cómo debe llevarse a cabo, y iii) informar al Tribunal de toda la labor de separación de lo necesario para comprobar las obligaciones fiscales, así como del resultado del copiado.

Por último, hace una comparativa con la STS de 14 de junio, dictada por el mismo Tribunal, por la que en un supuesto análogo se consideró no haberse vulnerado los derechos fundamentales a la inviolabilidad del domicilio y el secreto de las comunicaciones ni tampoco el principio de proporcionalidad siendo que el representante legal de la mercantil consintió la entrada en sus dependencias de los funcionarios intervinientes, incluyendo dicho consentimiento el acceso a los correos electrónicos. Además, la descarga de datos se limitó a un ordenador y a su servidor y no constaban datos de carácter personal o protegidos en dicha documentación.

En definitiva, la jurisprudencia opta para establecer cada vez un sistema más garantista en el mundo del entorno digital, donde el respeto a los derechos fundamentales debe primar sobre el ejercicio de potestades administrativas. Así, en un registro de medios TIC en el seno de una investigación interna, tanto la persona jurídica investigada como el trabajador, podrían negarse ante la AEAT o la propia empresa a colaborar al precinto y/o copiado de información cuando se encuentre en juego su derecho a la intimidad personal y al secreto de las comunicaciones sin que ello quepa entenderse como resistencia, obstrucción, excusa o negativa a las actuaciones de la Administración.

- **Sentencia de la Sala de lo social del Tribunal Supremo n.º 551/2023, de 12 de septiembre, p. Ureste García.**
  Temática: naturaleza y validez de la prueba obtenida por detective privado. En particular, sobre la (ir)relevancia de los indicios previos de incumplimiento laboral así como de la licitud de los seguimientos a trabajadores fuera del centro de trabajo.

En esta sentencia la Sala cuarta del Tribunal Supremo resuelve el recurso de casación por unificación de doctrina interpuesto por una empresa contra una sentencia de la Sala social del Tribunal Superior de Justicia del País Vasco, en la que confirmó la decisión de un Juzgado de lo Social de Bilbao consistente en declarar nulo el despido disciplinario en marzo de 2021 de un trabajador de la recurrente cuyo cese se basó, fundamentalmente, en la prueba obtenida por un detective privado.

Los hechos se refieren a un empleado con una larga antigüedad, computable desde 1993, dedicado a labores de limpieza en las instalaciones de los clientes de su empresa empleadora. En consecuencia, la mayor parte de su jornada laboral la pasaba fuera del centro de trabajo de la recurrente, desplazándose con un coche de la empresa junto con otro compañero.

Por comentarios recibidos de otros compañeros que prestaban servicios en los mismos entornos que el trabajador despedido, la empresa contrató un detective privado para hacer seguimiento del empleado durante su horario laboral. El profesional contratado concluyó que el trabajador incurría de forma regular y reiterada en conductas constitutivas de múltiples incumplimientos laborales, entre ellos varios de graves, como por ejemplo conducir el vehículo de la empresa bajo los efectos del alcohol, desempeñar sus tareas en estado de embriaguez, ausentarse de forma injustificada de su puesto de trabajo o hacer uso privativo de medios de la empresa.

Sobre la base del informe elaborado por el detective privado la empresa redactó carta de despido disciplinario y procedió a la rescisión del contrato. No se incluyeron ulteriores fuentes de prueba que corroboraran de manera sustancial los hechos objeto de la carta.

El Juzgado de los Social n.º 6 de Bilbao estimó la demanda interpuesta por el trabajador contra el despido disciplinario y lo declaró nulo, condenando además a la empresa a indemnizarle con 10.000,00 € en compensación por los daños morales causados con motivo de la lesión de su derecho fundamental a la intimidad. La Sala de lo social del Tribunal Superior de Justicia del País Vasco confirmó esta sentencia en lo sustancial.

El razonamiento del Juzgado y del Tribunal Superior de Justicia fue que la medida de seguimiento mediante detective privado fue desproporcionada y, por tanto, vulneradora del derecho fundamental a la intimidad (art. 18 CE) del trabajador porque la empresa había recurrido al detective sin contar con **indicios** sólidos de los presuntos incumplimientos laborales del trabajador.

La Sala de lo social del Tribunal Supremo estima el recurso de casación interpuesto por la empresa y declara expresamente, en reiteradas ocasiones, que ***«la clave del juicio de ilicitud*** *de la prueba no reside en la causa o motivo que la soporta. La concurrencia de ligeras sospechas, de meros indicios o de indicios relevantes no determinan la licitud o ilicitud de la prueba en sí misma considerada*» (negrita añadida). En esta línea, añade «[p]*or otra parte, la exigencia de indicios relevantes o sospechas fundadas llegaría a hacer inútil o superflua la adición de otros elementos probatorios*».

En su lugar, lo relevante es si la medida de investigación utilizada por el empresario ha supuesto una **intromisión** en la esfera de privacidad del trabajador. En tal caso habrá que determinar el grado de afectación y valorar si es conforme con el principio de proporcionalidad atendidas las circunstancias del caso. Al respecto se citan varios precedentes de la misma sala en los que se admite la prueba obtenida mediante seguimientos a pesar de no existir indicios previos de incumplimiento o de ser estos muy débiles.

Asimismo, se cita también otra resolución de la misma Sala cuarta del Tribunal Supremo, también de 2023, en la que se considera que la prueba obtenida es ilícita por haberse obtenido invadiendo un espacio reservado del trabajador, a saber, **el jardín** de su vivienda particular (*vid*. **STS Sala de lo social n.º 380/2023, de 25 de mayo).** Si bien en esta resolución se considera que el patio de un domicilio privado debe incardinarse en el concepto de "otro lugar reservado" según lo previsto en el **art. 48.3 de la Ley n.º 5/2014**, de 4 de abril, de Seguridad Privada, y, por tanto, vedado a la actividad indagatoria de los detectives privados, se añade expresamente que, en el caso particular, «*no consta que, en el presente supuesto, el jardín del trabajador fuera visible para cualquiera que pudiera pasar por su proximidad, ni que no hubiera muros, setos o vallas de cualquier naturaleza que dificultaran la visibilidad desde el exterior*», lo que lleva a pensar que, en el caso de que el jardín hubiera estado a la vista de cualquiera, quizá la conclusión habría sido distinta.

Por último, en la sentencia aquí comentada se recuerda la naturaleza probatoria del **informe de detective privado.** Como es sabido, no se trata de una prueba documental, sino de «*la plasmación por escrito de la prueba testifical sobre hechos observados por quien lo firma*». Se trata, por tanto, de una prueba personal «*que los Tribunales pueden valorar libremente, en función del conjunto de circunstancias concurrentes tanto desde el punto de vista de la legalidad de su intervención como desde el de la credibilidad de sus manifestaciones (STC 114/84)*».

- **Sentencia del Tribunal Superior de Justicia de Madrid, Sala de lo social, n.º 405/2023, de 8 de junio, p. Prieto Fernández.**
  Temática: control empresarial de las conversaciones de *Whatsapp* mantenidas por un trabajador a través del móvil corporativo. Alcance del derecho fundamental al secreto de las comunicaciones.

En fecha 6 de junio de 2023, la Sección 4ª de lo Social del Tribunal Superior de Justicia de Madrid se ha pronunciado acerca del secreto de las comunicaciones en el uso de redes sociales de comunicación como la conocida aplicación de WhatsApp a través de un dispositivo corporativo.

En la resolución se resuelve un recurso de suplicación interpuesto por la empresa demandada -junto a la impugnación de la adversa- contra la Sentencia dictada por el Juzgado de lo Social núm. 2 de Móstoles.

La trabajadora demandante fue despedida después de que su empleadora detectara, mediante herramientas informáticas, irregularidades en la gestión de cobro de pedidos de clientes. En concreto, la empresa demandada justificó el despido en base a conversaciones de WhatsApp mantenidas por la trabajadora a través del teléfono corporativo con un tercero no identificado, probablemente un cliente o un intermediario, relativas al cobro de comisiones, así como a los precios de compra y venta de productos.

Para seguir leyendo el comentario consúltese el siguiente enlace: https://www.molins.eu/control-empresarial-del-whatsapp-y-secreto-de-las-comunicaciones/