SUMARIO 2022 | INVESTIGACIONES INTERNAS

MOLINS

Defensa Penal

ÍNDICE

I**NTRODUCCIÓN**..... 4

1. **COMUNIDAD INTERNACIONAL**..... 6

International Organization for Standardization 6

 Proyecto de ISO 37008 – Guía para la conducción de investigaciones internas. 6

U.S. Securities and Exchange Commission..... 6

 Sanciones millonarias de la SEC por el uso sistemático de canales de comunicación informales con fines profesionales (*Whatsapp*, p.e.). 6

2. **EUROPA** 7

Tribunal de Justicia de la Unión Europea..... 7

Comisión Europea: cláusulas tipo en materia de transmisión internacional de datos 9

Comité Europeo de Protección de Datos: nace el primer sistema de certificación bajo el RGPD aprobado por el CEPD. 9

Estados miembros con la Directiva (UE) 2019/1937 traspuesta 10

3. **ESPAÑA**..... 13

Legislación 13

Jurisprudencia..... 14

Sentencia del **Tribunal Constitucional (Pleno)** n.º 119/2022, de 29 de septiembre, p. Narváez Rodríguez. 14

Sentencia del **Tribunal Constitucional** n.º 42/2022, caso OMNIUM CULTURAL 16

Temática: sanciones por transmisión internacional de datos personales. 16

Sentencia del **Tribunal Supremo (Pleno de la Sala de lo social)** n.º 692/2022, de 22 de julio, p. García-Perrote Escartín. 17

Sentencia del **Tribunal Supremo (Sala de lo penal)** n.º 132/2022, de 24 de enero, p. Hernández García. 18

Sentencia del **Tribunal Superior de Justicia de Madrid** n.º 671/2022, de 23 de septiembre, p. Moreno González-Aller: 18

Sentencia del **Tribunal Superior de Justicia** de Catalunya n.º 5693/2022, de 28 de octubre, p. Bono Romera: 19

Fiscalía General del Estado 19

INTRODUCCIÓN

Salvo en los EE.UU., la conducción de investigaciones empresariales internas no es una práctica asentada ni recurrente en la mayor parte de sistemas jurídicos del mundo. Su relevancia en la escena jurídico-económica suele estar a la estela de la existencia y del grado de implantación de los regímenes de responsabilidad penal de las personas jurídicas de los correspondientes países. Siendo la persecución penal de las empresas y otras organizaciones una tendencia político-criminal novedosa también en el plano internacional, no es de extrañar que la proliferación de este tipo de indagaciones aún esté en los albores.

Con todo, el año 2022 ha dado algunos frutos relevantes en este proceso de maduración. En el plano internacional resulta destacable el proyecto de Guía para la conducción de investigaciones internas desarrollada por la *International Organization for Standardization* (proyecto de ISO/DTS 37008).

En Europa, el pasado año ha venido marcado por la finalización del plazo concedido a los Estados miembros de la Unión Europea para implementar la Directiva (UE) 2019/1937, de 23 de octubre, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Los Estados tenían hasta el 17 de diciembre de 2021 para aprobar la normativa de trasposición. El mandato europeo consiste en imponer el deber de establecer canales de denuncia interna y sistemas de protección del delator (*whistleblower*) frente a posibles represalias a las entidades del sector público y a las del sector privado con más de 250 trabajadores. Las entidades más pequeñas, de menos de 250 trabajadores, pero con más de 50, también están en el punto de mira, pero respecto de ellas el plazo de implementación se extiende hasta el 17 de diciembre de este año 2023.

A día de hoy el plazo no ha sido observado por un número importante de Estados, entre los que se cuentan Alemania, Italia, Austria, Polonia y España. Entre los que pueden presumir de más puntualidad están Francia y Portugal.

Del viejo continente también cabe destacar la finalización del plazo para adaptarse a la Decisión de la Comisión sobre cláusulas tipo en materia de transferencia internacional de datos, cuestión sensible en cualquier investigación transfronteriza, así como el primer sistema de certificación aprobado por el Comité Europeo de Protección de Datos respecto de las medidas exigidas por el RGPD. A nivel jurisdiccional debe mencionarse la Sentencia del Pleno del Tribunal de Justicia de la Unión Europea sobre el alcance del deber de secreto profesional de los abogados, a raíz de las obligaciones de comunicación de información a las autoridades sobre operaciones fiscales de riesgo impuestas por la DAC 6 (Directiva dirigida a prevenir el fraude fiscal). La preservación de los resultados de las investigaciones frente a su requerimiento o incautación por parte

de las autoridades públicas depende, entre otras cosas, del alcance conferido al deber de secreto profesional, por lo que la postura adoptada por el Pleno del TJUE sobre este derecho/deber, aunque sea en otros ámbitos, resulta necesariamente de interés.

Por lo que se refiere a España, aparte de la aprobación del proyecto de Ley de protección de los informantes, destacan varias sentencias de nuestros Tribunales en materia de validez de las fuentes de prueba obtenidas mediante sistemas de grabación de la imagen y/o de la voz, o mediante registros de aparatos informáticos y/o de telecomunicación. Entre ellas se encuentra una sentencia dictada por el Pleno del Tribunal Constitucional, que se dividió en dos bloques opuestos a raíz de la problemática enjuiciada: el alcance del deber de informar de manera específica a los trabajadores de la existencia de un sistema de video-vigilancia. El fallo cuenta con cinco votos particulares de los once emitidos.

También está una sentencia del Pleno de la Sala de lo social del Tribunal Supremo, sobre la misma problemática. En este caso el fallo se dictó por unanimidad.

Que en un solo año recaigan dos resoluciones de plenos y una con el voto particular de la mitad menos uno de los integrantes del Tribunal es muestra de que la cuestión tratada es tan relevante como controvertida.

Con la esperable aprobación de las normativas nacionales en materia de protección de los denunciantes (*whistleblowers*) de los estados miembros que aún no han traspuesto la Directiva 2019/1937, incluida España, y con la probable publicación de la ISO 37008, sobre conducción de investigaciones internas, cabe avanzar que en el año 2023 se darán firmes e importantes pasos hacia adelante en la progresiva normalización de las investigaciones empresariales internas en el ámbito jurídico-económico. Estaremos expectantes.

En Barcelona, a 6 de febrero de 2023.

Equipo de Investigaciones Internas
Molins Defensa Penal

1. COMUNIDAD INTERNACIONAL

Del pasado año 2022, en el plano internacional, destacan el proyecto de guía sobre investigaciones internas de la *International Organization for Standardizaton* y la sanción millonaria impuesta por la SEC a 16 empresas de inversión en la bolsa de *Wall Street* por el uso sistemático de aplicaciones de mensajería informales (*Whatsapp*, p.e.) para fines profesionales.

International Organization for Standardization

- Proyecto de ISO 37008 – Guía para la conducción de investigaciones internas.

El proyecto de **ISO/DTS 37008**, actualmente en fase de desarrollo, consiste en una guía sobre la conducción de investigaciones internas dirigida a cualquier tipo de organización, sea del sector público, privado o de beneficencia (ONGs, fundaciones, asociaciones, etc.).

Su objetivo es proporcionar orientación a las entidades para identificar mejor qué ha ocurrido, por qué ha ocurrido (causa raíz), así como para decidir quién debería llevar a cabo la investigación, cómo debería llevarla a cabo, qué medidas correctoras adoptar, qué y cómo denunciar y cómo prevenir eventuales represalias.

El proyecto de guía se encuentra en un estadio avanzado del proceso de tramitación. Ha superado las fases de propuesta, preparación y estudio del proyecto en comité, así como el periodo de consultas. Actualmente se encuentra en fase de aprobación. Una vez convalidado el siguiente paso será su publicación[1].

U.S. Securities and Exchange Commission

- Sanciones millonarias de la SEC por el uso sistemático de canales de comunicación informales con fines profesionales (*Whatsapp*, p.e.).

La normativa de los EE.UU. reguladora de los mercados financieros obliga a las entidades de inversión autorizadas para operar en la bolsa de *Wall Street* a registrar y conservar todas las comunicaciones mantenidas por sus empleados en el marco de su actividad profesional.

Tras la correspondiente indagación, la autoridad de los mercados financieros estadounidense, la *U.S. Securities and Exchange Commission* (SEC), llegó a la conclusión de que los empleados de dieciséis de estas empresas, entre los que se

[1] Se puede ver el detalle del procedimiento en https://www.iso.org/stage-codes.html#50_00.

incluían altos directivos, habían estado usando de forma sistemática aplicaciones de mensajería informales (*Whatsapp*, p.e.) respecto de las cuales las respectivas empresas no guardaban el debido registro de comunicaciones ni efectuaban la supervisión exigida.

Dieciséis entidades aceptaron los hechos imputados y llegaron a un acuerdo con el regulador. Entre ellas están BARCLAYS CAPITAL INC., MERRILL LYNCH, CITIGROUP GLOBAL MARKETS INC., CREDIT SUISSE SECURITIES (USA) LLC, DEUTSCHE BANK SECURITIES INC., GOLDMAN SACHS & CO. LLC, MORGAN STANLEY & CO. LLC y UBS SECURITIES LLC. La multa impuesta a cada una de las mencionadas asciende a **125 millones de dólares.** El acuerdo alcanzado incluye la monitorización del proceso de adecuación a la normativa financiera.

2. EUROPA

Tribunal de Justicia de la Unión Europea

Pocos días antes de que finalizara el año 2022 se publicó la Sentencia del Pleno del Tribunal de Justicia de la Unión Europea en el asunto C-694/20, cuyo objeto era una cuestión prejudicial sobre la compatibilidad con el derecho a la vida privada (art. 7 de la Carta de Derechos Fundamentales de la UE) de las obligaciones de comunicación de información a terceros impuestas a los abogados por la Directiva DAC 6.

En el marco de las políticas y medidas de prevención del fraude fiscal adoptadas por las instituciones de la Unión, en el año 2018 se aprobó la Directiva (UE) 2018/822, también conocida como DAC 6, en la que se obliga a los Estados miembros a establecer determinados deberes de comunicación a los abogados que, de algún modo, intervengan en el diseño, comercialización, organización, puesta a disposición para su ejecución o gestión de la ejecución de un mecanismo transfronterizo de planificación fiscal potencialmente agresivo, sujeto a comunicación de acuerdo con la normativa DAC.

Si bien la normativa DAC exime a los intermediarios sujetos al deber de secreto profesional de la obligación de informar a las autoridades públicas competentes, en el art. 8 bis ter de la DAC 6 se obliga a los Estados miembros a imponer a tales intermediarios, entre los que se cuentan los abogados, el deber de informar a los demás intermediarios que participen en la configuración o ejecución del mecanismo de planificación fiscal potencialmente agresivo de que, debido a su deber de secreto profesional, no van a cumplir con la obligación de comunicación prevista en la DAC.

Como pone de manifiesto el Tribunal, este deber implica una doble injerencia en el derecho al secreto de las comunicaciones entre abogado y cliente, contenido en el derecho a la vida privada previsto en el art. 7 de la CDFUE. En primer lugar, el derecho se ve afectado por el hecho de que el abogado tenga que comunicar a un tercero la existencia de la consulta o asesoramiento prestado al cliente, su valoración de que la misma hace referencia a un mecanismo de planificación fiscal potencialmente agresivo, así como su identidad. La segunda injerencia, indirecta, consiste en la comunicación que el intermediario está obligado a realizar a las autoridades tributarias sobre la identidad del abogado que ha informado de su dispensa, así como de la existencia de la consulta del cliente.

Apreciada la existencia de esta doble injerencia en el derecho fundamental, el Pleno del TJUE examina si la afectación está justificada. En aplicación del test de proporcionalidad concluye que, si bien la medida es idónea para maximizar la prevención del fraude fiscal (fin legítimamente perseguido), es innecesaria para garantizar que las administraciones tributarias tengan conocimiento de la existencia de un mecanismo transfronterizo de planificación fiscal potencialmente agresiva. Pues tanto los demás intermediarios como el cliente, cuando no existan intermediarios obligados a informar, tienen el deber de comunicar la existencia del mecanismo a las autoridades. Por tanto, el deber impuesto a los abogados en virtud de la DAC 6 no es imprescindible para que las administraciones tributarias puedan tener conocimiento del mecanismo.

La Sentencia resuelve una cuestión prejudicial planteada por el Tribunal Constitucional belga en relación con su normativa de trasposición de la DAC 6. En España la normativa de trasposición, integrada por la Ley 10/2020, de 29 de diciembre, el Real Decreto 243/2021, de 6 de abril, y la Orden HAC/342/2021, de 12 de abril, se encuentran recurridas ante el Tribunal Supremo y la Audiencia Nacional por parte de la Asociación Española de Asesores Fiscales. Al igual que en Bélgica, la citada normativa española imponía a los abogados los deberes de comunicación comentados bajo amenaza de sanciones pecuniarias, en fiel cumplimiento de lo mandado por el legislador europeo. A la luz de la Sentencia del Pleno del TJUE cabe esperar que este deber será derogado.

La resolución resulta importante en materia de investigaciones internas en la medida en que es un reflejo de la posición del Pleno del Tribunal de Justicia de la Unión Europea en relación con el alcance del deber de secreto de las comunicaciones entre el abogado y su cliente. Es esta una cuestión especialmente delicada en el ámbito de las

investigaciones internas, en el que a la luz de la praxis estadounidense y de la conocida Sentencia del Tribunal Constitucional alemán de 2018 plana el temor de que las autoridades públicas competentes puedan requerir o incautar los resultados de una investigación interna.

Comisión Europea: cláusulas tipo en materia de transmisión internacional de datos

El pasado 27 de diciembre de 2022 finalizó el periodo transitorio para modificar las cláusulas contractuales tipo en materia de transferencia internacional de datos personales.

Actualmente deben emplearse las cláusulas tipo previstas en la **Decisión de la Comisión Europea 2021/914**, bajo riesgo de incurrir en sanciones por incumplimiento de la normativa de protección de datos contenida o derivada del Reglamento General de Protección de Datos.

Comité Europeo de Protección de Datos: nace el primer sistema de certificación bajo el RGPD aprobado por el CEPD.

La autoridad competente en materia de protección de datos en Luxemburgo, la *Commission nationale pour la protection des données* (CNPD), ha desarrollado el primer sistema de certificación bajo el Reglamento General de Protección de Datos (RGPD) aprobado por el Comité Europeo de Protección de Datos (CEPD — EDPB, en inglés).

El CEPD es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades nacionales competentes de esta materia en la UE.

El sistema de certificación desarrollado por la autoridad luxemburguesa, denominado GDPR-CARPA, se basa en un informe ISAE 3000 Tipo 2, el cual permite emitir una opinión sobre la correcta implementación del mecanismo de control con la asunción de responsabilidades formales por parte del auditor.

Dado que es un sistema desarrollado y aplicado por la autoridad de protección de datos de Luxemburgo tan solo pueden optar a esta certificación las entidades que operen en este país. No obstante, constituye un referente para las autoridades nacionales del resto de estados miembros de la Unión Europea, que de bien seguro seguirán los pasos de su homóloga luxemburguesa.

Estados miembros con la Directiva (UE) 2019/1937 traspuesta

Hasta la fecha dieciséis (16) estados miembros han aprobado ya la normativa nacional de trasposición de la Directiva reguladora del *Whistleblowing*, diez (10) han iniciado los trámites legislativos, sin haber llegado a aprobar la norma de implementación y uno (1) aún no ha iniciado el proceso de tramitación legislativa (Hungría)[2].

Entre los Estados impuntuales se cuentan Austria, Polonia, Italia, Alemania y España. En la lista de los más disciplinados figuran, entre otros, Dinamarca, Finlandia, Suecia, Bélgica, Grecia, Irlanda, Holanda, Francia y Portugal.

La Directiva obliga a los Estados miembros a aprobar las disposiciones normativas nacionales que sean necesarias para imponer a las entidades del sector público y a las del sector privado con más de 50 trabajadores el deber de establecer canales internos de denuncia, así como adoptar medidas para proteger a los delatores frente a represalias, en relación con determinadas infracciones del Derecho de la Unión. Ello sin perjuicio de que los Estados miembros puedan extender tales deberes a denuncias sobre infracciones de Derecho interno, internacional o de otro ámbito.

El legislador europeo obliga a que los canales internos de denuncia y las medidas de protección no solo estén disponibles para los empleados de las entidades afectadas, sino también para ex empleados, personas del entorno del informante o periodistas.

Un aspecto muy importante de la Directiva es que obliga a conferir protección a los delatores independientemente de que su primera comunicación no haya sido a través del canal interno de la entidad afectada. El legislador europeo exige que el informante pueda escoger entre el sistema de denuncia interno o el externo, consistente en los canales habilitados por la autoridad pública competente. La comunicación pública (a través de medios de comunicación) también debe ser posible en primera instancia, pero en este caso deben cumplirse determinadas condiciones: o bien haber tratado de agotar los canales interno o institucional, o bien que exista un interés público acuciante (art. 15).

Por último, se ordena a los Estados miembros a imponer sanciones efectivas, proporcionadas y disuasorias a las personas físicas o jurídicas que: i) dificulten la interposición de denuncias; ii) tomen represalias contra los denunciantes; iii) no preserven la confidencialidad del denunciante (art. 23).

En lo que sigue se hace una breve mención a los aspectos más destacables de dos de los Estados miembros que ya han cumplido con el deber de trasposición. Por razones

[2] Véase la página web: https://www.whistleblowingmonitor.eu/.

de proximidad geográfica y comercial se ha prestado atención al régimen aprobado en Francia y en Portugal.

- Francia:

Aprobada el 21 de marzo de 2022, la Loi n.º 2022-401, dirigida a mejorar la protección de los alertadores, también conocida como "Ley Waserman", entró en vigor el pasado 1 de septiembre para todas las entidades, públicas o privadas, con más de 50 empleados.

Francia ya contaba con un régimen de protección de los delatores antes de la aprobación de la Directiva (UE) 2019/1937. Se trata de las previsiones contenidas en la "Ley Sapin II" (Loi n.º 2016-1691).

La nueva Ley de 2022 ha reformado en aspectos sustanciales el régimen previsto en la "Ley Sapin II", en la que el legislador francés adoptaba una posición más equilibrada entre los intereses del denunciante, los de la generalidad y los del denunciado. Para cumplir con las exigencias de la Directiva (UE) 2019/1937 es preciso un modelo más centrado en los intereses del informante y los de la comunidad. En este sentido, la Loi n.º 2022-401 ha derogado el anterior protocolo de tres pasos que debía seguir el denunciante: 1) primero recurrir al sistema de denuncia interna de la entidad; 2) Luego, en el supuesto de que la denuncia interna no se tramitara adecuadamente, recurrir al sistema de denuncia institucional externa; 3) como último recurso, proceder a la difusión pública del hecho. Ahora, tras la reforma, el delator puede elegir libremente entre el sistema de denuncia interna o el institucional externo. La difusión pública es también una opción, pero sujeta a mayores condiciones. Todo ello de acuerdo con lo previsto en la Directiva.

En cuanto al tipo de infracciones denunciables, el legislador francés ha ampliado el objeto de las denuncias a: i) cualquier delito o falta; ii) amenazas o daños al interés general; violaciones o intentos de ocultar violaciones de compromisos internacionales ratificados o aprobados por Francia, o actos unilaterales de una organización internacional basados en tales compromisos; iv) violaciones de la Ley o de la normativa de la Unión Europea.

Resultan también interesantes los incentivos previstos a favor de los informantes. Se les exime de responsabilidad penal respecto de las apropiaciones indebidas, sustracciones u ocultaciones de documentos relacionados con el objeto de la denuncia a los que hayan accedido de forma legítima. También se les exonera de la responsabilidad civil por los daños o perjuicios que pueda haber causado la denuncia presentada de buena fe.

En materia de sanciones el legislador francés ha previsto una multa civil de 60.000 € por las actuaciones dilatorias o abusivas de las entidades afectadas, dirigidas a dificultar o

a ocultar la denuncia. Quienes discriminen o tomen represalias contra el alertador pueden ser condenados a 3 años de prisión y multa de 45.000 €.

- Portugal:

En el país luso la Directiva (UE) reguladora del Whistleblowing fue traspuesta a través de la Lei n.º 93/2021, sobre el régimen general de protección de los denunciantes de infracciones. Entró en vigor el pasado 18 de junio de 2022.

En Portugal ya existían un buen número de normas sectoriales que imponían a determinadas empresas y entidades el deber de contar con canales de denuncia interna y otras medidas previstas en la Directiva. La Lei n.º 92/2021 no deroga tales regímenes específicos, sino que actúa como norma general subsidiaria.

Desde junio de 2022 todas las entidades del sector público o privado con más de 50 empleados, así como los municipios con más de 10.000 habitantes, deben contar con canales internos de denuncia.

Del régimen luso destaca la priorización de los canales de denuncia disponibles para el informante. El legislador portugués condiciona las medidas de protección a que el delator haya seguido el siguiente orden: 1) primero recurrir al canal interno de denuncias; 2) en segundo lugar recurrir a los canales institucionales externos, si a nivel interno no se ha recibido una respuesta adecuada; 3) en última instancia se permite difundir públicamente los hechos.

En materia de sanciones se distingue entre faltas muy graves y graves, así como entre las infracciones cometidas por personas jurídicas y las atribuibles a personas físicas:

Faltas muy graves *Ejemplos*: impedir la presentación o seguimiento de una denuncia; represalias; vulneración del deber de confidencialidad.	Personas físicas: 1.000 € a 25.000 € Personas jurídicas: 10.000 € a 250.000 €
Faltas graves *Ejemplos*: no establecer canales de denuncia interna; incumplir con las garantías de los canales (independencia, imparcialidad).	Personas físicas: 500 € a 12.500 € Personas jurídicas: 1000 € a 25.000 €

3. ESPAÑA

Legislación

El pasado 23 de septiembre de 2022 fue publicado el **Proyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción** por la que se transpone la Directiva (UE) 2019/1937 reguladora del *Whistleblowing*.

El proyecto de Ley español amplía el ámbito de aplicación de la Directiva. Las infracciones que pueden comunicarse a través de los canales de denuncia previstos por la norma proyectada y que dan derecho a las medidas de protección en ella previstas son las que siguen:

- Infracciones del Derecho de la Unión Europea previstas en la Directiva 2019/1937, infracciones que afecten a los intereses financieros de la UE, así como infracciones que incidan en el mercado interior.
- Infracciones penales
- Infracciones administrativas graves o muy graves.

En el ámbito subjetivo, los canales de información internos pasan a ser obligatorios para las **empresas privadas** que cuenten con **más de 50 trabajadores**. Se incluyen los partidos políticos, sindicatos y organizaciones empresariales, así como las fundaciones creadas por estos, siempre que reciban o gestionen fondos públicos.

Asimismo, se extiende la obligación a todas las entidades del **sector público**, salvo los municipios de menos de 10.000 habitantes o con menos de 50 trabajadores.

El Proyecto de ley exige a las empresas permitir las **comunicaciones anónimas** (art. 7.3). Las denuncias a través de los canales institucionales externos también pueden ser de carácter anónimo (art. 17.1)

En el proyecto se indica expresamente que el **canal interno** será el preferente (art. 4.1). No obstante, en el capítulo regulador de los **canales externos** se establece que el informante puede recurrir a él después de agotar la vía interna o directamente. Salvo que la mención al carácter preferente del canal interno sea una mera declaración de intenciones sin efectos normativos vinculantes, estamos ante una evidente

contradicción interna que debería resolverse durante la tramitación legislativa del proyecto, pues afecta a un aspecto fundamental del fenómeno de la delación. La Directiva parece exigir libertad de elección entre el canal interno y el institucional externo, tal y como prevé la regulación francesa, pero es cierto que países como Portugal establecen una priorización a favor del sistema interno. Veremos si la compatibilidad de este segundo modelo con la Directiva se ve cuestionada ante el TJUE en el futuro próximo.

Se establece un **régimen sancionador** que, en su artículo 63, clasifica las infracciones en "muy graves", "graves" o "leves". Conviene advertir que los **sujetos responsables** pueden ser tanto las entidades (personas jurídicas) como las personas físicas que las integran, incluso después de finalizada la relación laboral o contractual con la empresa afectada (art. 62.3).

Ejemplo de infracción muy grave es el incumplimiento de la obligación de disponer de un sistema interno de información, pudiendo ser objeto de sanción con una multa que oscile entre 600.001 y **1.000.000 euros** para las personas jurídicas y entre 30.001 y **300.000 euros** para las personas físicas. En comparación con los regímenes sancionadores de Francia y Portugal el proyecto de Ley español es, sin duda, muchísimo más severo (véase comentario *supra*).

Jurisprudencia

Sentencia del **Tribunal Constitucional (Pleno)** n.º 119/2022, de 29 de septiembre, p. Narváez Rodríguez.
Temática: validez probatoria de imágenes captadas por sistema de video-vigilancia.

El Pleno del Tribunal Constitucional conoció la demanda de amparo interpuesta por un empresario al que se le inadmitió como fuente de prueba válida en un proceso laboral por despido disciplinario la grabación obtenida por su sistema de video-vigilancia sobre una determinada actuación del empleado despedido.

En las imágenes se ponía de manifiesto que el trabajador se apropiaba de bienes de la empresa y posteriormente los enajenaba a terceros quedándose con el dinero. La inadmisión de la prueba conllevó la declaración del despido como improcedente, por descansar la base probatoria sobre las imágenes de vídeo.

La razón de la inadmisión esgrimida por el Tribunal Superior de Justicia del País Vasco fue que el empresario no había cumplido con su deber «*de informar con carácter previo,*

y de forma expresa, clara y concisa» a los trabajadores de la existencia del sistema de video-vigilancia y de su uso con la finalidad de controlar su desempeño laboral, deber previsto por el art. 89.1 de la Ley Orgánica de Protección de Datos (LOPD, en adelante).

El empleador sí había cumplido con el deber general de informar de la existencia de cámaras mediante el cartel visible homologado por la Agencia Española de Protección de Datos (*vid*. art. 22.4 LOPD e Instrucción n.º 1/2006 de la AEPD). Por ello el empresario invocó la excepción prevista por el segundo párrafo del art. 89.1 LOPD: «[e]*n el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica*».

Sin embargo, el TSJ del País Vasco desestimó su aplicación porque era la segunda vez que el demandante de amparo recurría a su sistema de video-vigilancia para despedir a un empleado. Cinco años antes ya había recurrido a él en un caso similar. El Tribunal entendió la falta de regularización de la situación en relación con el deber de informar de forma específica a los trabajadores como *«una interpretación unilateral de la facultad excepcional, atribuyéndose medios y facultades que el Ordenamiento Jurídico solo ha previsto de forma excepcional y que en modo alguno sirven para omitir los deberes que frente a los derechos fundamentales competen a la empresa*».

El Pleno del Tribunal Constitucional estimó la demanda de amparo del empresario, anulando la Sentencia del TSJ del País Vasco, por entender que la excepción del párrafo segundo del art. 89.1 LOPD era aplicable, a pesar de los antecedentes del empresario. Lo relevante, según la mayoría del Pleno, es que el empleado haya incurrido en una conducta ilícita y que el sistema le haya captado *in fraganti*. Que el empresario haya tenido necesidad de recurrir al sistema de video-vigilancia en ocasiones previas no afecta en absoluto a los dos únicos criterios relevantes: a) que el trabajador haya cometido un hecho ilícito, y b) que las cámaras lo hayan captado en plena ejecución (flagrancia).

Esta sentencia cuenta con el voto particular de 5 de los 11 magistrados que integraban el Pleno en el momento en que fue dictada. Entre ellos están el actual Presidente, el Excmo. Sr. Conde-Pumpido, la actual Vice-Presidenta, la Excma. Sra. Montalbán, así como el Excm. Sr. Sáez y la Excma. Sra. Balaguer. En su opinión, la mayoría estaría «*poniendo en un mismo nivel valorativo la regla general y la excepción*». Si de ellos depende: «[n]*o bastará que se verifique que concurre una situación de flagrancia en la captación de la imagen y la presencia en el lugar de trabajo de los carteles anunciadores de la existencia del sistema para legitimar, desde la perspectiva del art. 18.4 CE, el uso de esa imagen con fines disciplinarios. Será preciso, además, en atención a la naturaleza esencial y principal del deber específico de información a los trabajadores en*

cuanto garantía del derecho fundamental, que se den cumplidas razones por parte del empleador respecto de su incumplimiento».

Habiendo cambiado sustancialmente la composición del Pleno no cabe descartar que la postura minoritaria en la fecha de esta resolución se imponga en un futuro, en una sentencia sobre un asunto nuevo similar.

Sentencia del **Tribunal Constitucional** n.º 42/2022, caso OMNIUM CULTURAL
Temática: sanciones por transmisión internacional de datos personales.

En esta resolución el Tribunal Constitucional desestima el recurso de amparo interpuesto por ÒMNIUM CULTURAL contra la Sentencia de la Sala contencioso-administrativa de la Audiencia Nacional, en la que se confirma la sanción por importe de **90.000 €** impuesta por la Agencia Española de Protección de Datos contra la entidad.

En julio de 2014 la asociación ÒMNIUM CULTURAL firmó un contrato con la mercantil BLUE STATE DIGITAL, Inc. (BSD), para que esta empresa, en calidad de responsable del fichero, almacenara un archivo de la entidad con numerosos datos personales en sus servidores sitos en los EE.UU..

En el momento de suscripción del contrato la transferencia internacional de datos estaba amparada por la Decisión de la Comisión 2000/520/CE, según la cual los EE.UU. eran considerados un "puerto seguro" (*safe harbour*) para alojar datos personales de ciudadanos europeos.

Sin embargo, en su Sentencia de 6/10/2015, el Tribunal de Justicia de la Unión Europea invalidó la Decisión de la Comisión mencionada en lo que se refiere a la consideración de los EE.UU. como puerto seguro en materia de protección de datos.

Si bien ÒMNIUM CULTURAL trató de rescindir el contrato con BSD durante los meses posteriores a la publicación de la Sentencia del TJUE, haciéndose efectiva la extinción del contrato y la eliminación del fichero en septiembre de 2016, la AEPD le impuso una sanción de 90.000 € por haber incumplido la prohibición prevista en el art. 33 LOPD (versión de 1999, vigente en el momento de los hechos).

La Agencia había recibido la denuncia de dos particulares en abril de 2016 y, tras iniciar expediente sancionador contra ÒMNIUM, detectaron que la entidad no había marcado

el campo relativo a transferencias internacionales de datos en el Registro General de Protección de Datos, a pesar de que en su día habían inscrito el archivo en cuestión. Asimismo, la Agencia reprochó a la entidad que no le informara de la existencia de un fichero en los EE.UU. tras la publicación de la Sentencia del TJUE, pese a que el 19/10/2015 la AEPD publicó en su página web un comunicado informando de los efectos de la sentencia.

La sanción impuesta a ÒMNIUM fue la segunda aplicada por la AEPD por un incumplimiento en materia de transferencia internacional de datos.

Sentencia del **Tribunal Supremo (Pleno de la Sala de lo social)** n.º 692/2022, de 22 de julio, p. García-Perrote Escartín.
Temática: validez probatoria de una cámara oculta instalada por la empleadora.

En esta sentencia el Pleno de la Sala de lo social del Tribunal Supremo estima el recurso de casación interpuesto por una empleadora del hogar a la que el Tribunal Superior de Justicia de Asturias había inadmitido como prueba válida las imágenes captadas por la cámara oculta instalada en su domicilio, con la consecuente improcedencia del despido de su trabajadora doméstica.

A la propietaria de la vivienda le habían sustraído 30.000 € en metálico, una caja con joyas y otros objetos de valor ubicados en el armario de su habitación y otras estancias de la casa. Tras el incidente instaló una cámara oculta delante del armario donde tenía la caja fuerte. Semanas más tarde, revisando las imágenes captadas, comprobó que su empleada del hogar había intentado forzar la caja fuerte.

La empleadora del hogar, que tenía a varias personas que la ayudaban por ser tetrapléjica, no informó a sus empleados de forma específica sobre la (posible) existencia de cámaras. Tampoco instaló el cartel homologado por la AEPD (*vid*. art. 22.4 LOPD e Instrucción n.º 1/2006 de la AEPD).

La Sala cuarta entendió que, en este caso particular, la medida era proporcionada, por lo que no considera vulnerado el derecho fundamental a la protección de los datos personales de la empleada (art. 18.4 CE). Entre los múltiples argumentos empleados para fundamentar su decisión destaca uno. Según la Sala se debe distinguir entre sistemas de video-vigilancia permanentes y puntuales. En los primeros el cumplimiento del deber genérico de informar con el cartel homologado (art. 22.4 LOPD) es prácticamente ineludible. En las instalaciones puntuales, este deber admite mayor relativización.

Sentencia del **Tribunal Supremo (Sala de lo penal)** n.º 132/2022, de 24 de enero, p. Hernández García.
Temática: validez probatoria de la prueba obtenida mediante el registro del correo electrónico corporativo.

En esta resolución la Sala de lo Penal del Tribunal Supremo afianza la doctrina establecida en sus Sentencias n.º 489/2018, de 23 de octubre, p. del Moral García y n.º 328/2021, de 22 de abril, p. Marchena Gómez, en las que se examinan las condiciones en las que un empresario puede acceder al correo electrónico de un empleado de forma legítima.

El acceso al correo electrónico del trabajador solamente es lícito si se cuenta con el consentimiento previo del trabajador. Su anuencia puede ser expresa o tácita. En todo caso, es imprescindible un **anuncio previo** de la posibilidad de inspección de los aparatos y sistemas informáticos y/o telemáticos puestos a disposición del empleado. La advertencia debe determinar con claridad y precisión las condiciones del eventual registro: «*quién, cómo, cuándo, por qué y con qué alcance*» se puede producir el acceso.

El caso presenta una particularidad destacable: la persona que accedió a los correos electrónicos fue un **socio** de la mercantil. Obviamente la parte adversa cuestionó la legitimidad de su acceso por el simple hecho de carecer de competencias para ello. Si bien la Sala no entró en el fondo con un pronunciamiento sobre este extremo, sí manifestó que «*resulta*[a] *muy discutible que la mera condición de socio de una mercantil, sin atribución de responsabilidad gestora alguna, habilite para ejercer funciones de control y supervisión de la actividad empresarial, fuera de los cauces del derecho a la información que garantiza la legislación sectorial*».

Sentencia del **Tribunal Superior de Justicia de Madrid** n.º 671/2022, de 23 de septiembre, p. Moreno González-Aller:
Temática: validez probatoria de la grabación de una conversación telefónica entre dos trabajadores obtenida por el empresario.

El Tribunal Superior de Justicia de Madrid conoció el caso de un empresario que, en el marco de un procedimiento laboral por despido, aportó la grabación de la conversación telefónica mantenida por el trabajador cesado con otro compañero, en la que el primero insultaba y amenazaba al segundo.

Del texto de la Sentencia se infiere que la grabación fue obtenida por la empresa, no por el trabajador insultado y amenazado. Sin embargo, fue este quien denunció lo ocurrido

a sus superiores, estando de acuerdo en que la mercantil usara la grabación como fuente de prueba en los procedimientos judiciales que su empleadora tuviera frente al otro trabajador. El consentimiento de la grabación por parte de uno de los interlocutores se habría producido *ex post*.

Sin explayarse en el examen de proporcionalidad de la medida adoptada por la empresa, el Tribunal concluye que la prueba es válida, por lo que confirma la sentencia de instancia, desestimatoria de la demanda del trabajador por despido improcedente.

Sentencia del **Tribunal Superior de Justicia** de Catalunya n.º 5693/2022, de 28 de octubre, p. Bono Romera:
Temática: validez de la prueba obtenida por el empresario de las redes sociales del trabajador.

El Tribunal Superior de Justicia de Catalunya se pronuncia en esta resolución sobre la posibilidad de que un empresario utilice como fuente de prueba válida en un procedimiento laboral las fotografías que, de sí misma, haya podido colgar una empleada en su cuenta personal de *Facebook*.

La Sala de lo Social del TSJ de Catalunya confirma la admisibilidad de la prueba con el argumento de que la empleada habría realizado un acto de liberalidad respecto de las fotografías personales colgadas en la red social, sin restricción alguna a sus contactos, a quienes permite el acceso a su perfil, sobre su eventual uso o difusión.

Fiscalía General del Estado

El 20 de diciembre de 2022 la Fiscalía General del Estado publicó la Circular n.º 2/2022, sobre la actividad extraprocesal del Ministerio Público en el ámbito de la investigación penal, revisando y actualizando los criterios previstos sobre la materia en la Circular n.º 4/2013, sobre Diligencias de Investigación.

En lo que aquí interesa cabe destacar tres apartados de la Circular. El relativo al tratamiento debido a las denuncias anónimas (punto 4.2.3), el referido a la admisibilidad de las pruebas obtenidas por particulares (punto 5.9) y el dedicado al aseguramiento de los datos o informaciones incluidos en sistemas informáticos, como medida cautelar (punto 7.2.).

- Denuncias anónimas (punto 4.2.3)

En palabras de la Fiscalía General del Estado, con independencia de las irregularidades de naturaleza formal que puedan concurrir en la denuncia formulada ante el Ministerio Fiscal, nada impedirá su admisión a trámite y la consiguiente incoación de las oportunas diligencias de investigación cuando los hechos de apariencia delictiva comunicados presenten indicios de verosimilitud.

- Admisibilidad de pruebas obtenidas por particulares (punto 5.9)

Respecto de la validez de la prueba obtenida por particulares la Fiscalía hace suya la doctrina sentada por el Pleno del Tribunal Constitucional en la STC n.º 97/2019 (asuntos *Falciani*).

La instrucción dirigida a los integrantes del Ministerio Público es que la prueba obtenida por el particular vulnerando derechos fundamentales no debería ser, por regla general, admitida. No obstante, a la luz de la doctrina sentada por el Pleno del Tribunal Constitucional, los Fiscales deberán valorar la conveniencia de tenerlas en cuenta sobre la base de los siguientes parámetros:

> i) La índole y características de la infracción, ponderando su conexión instrumental, objetiva o subjetiva con la investigación desarrollada por las autoridades públicas.
>
> ii) El resultado de la actuación y, en concreto, su mayor o menor incidencia en el núcleo esencial del derecho violentado.
>
> iii) El riesgo de propiciar prácticas que comprometan pro futuro la efectividad del derecho fundamental en juego para el supuesto de admitirse la valoración en el caso concreto de la prueba, es decir, su posible efecto llamada.

Particularmente interesante resultan las indicaciones contenidas en relación con las grabaciones de conversaciones privadas. Se reproducen literalmente, por su especial interés:

> a) La utilización en el proceso penal de grabaciones de conversaciones privadas realizadas por uno de los interlocutores no vulnera el derecho al secreto de las comunicaciones.

b) Tampoco vulnera el derecho a la intimidad, salvo casos excepcionales en los que el contenido de la conversación afectase al núcleo de la intimidad personal o familiar de uno de los interlocutores.

c) Las grabaciones realizadas desde una posición de superioridad institucional (agentes de la autoridad o superiores jerárquicos) para obtener una confesión extraprocesal arrancada mediante engaño vulneran el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable y, en consecuencia, incurren en nulidad probatoria.

d) Las grabaciones realizadas en el ámbito particular no vulneran el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable.

e) Puede vulnerar el derecho a un proceso con todas las garantías aquella grabación en la que la persona ha sido conducida al encuentro utilizando argucias con la premeditada pretensión de hacerle manifestar hechos que pudieran ser utilizados en su contra, en cuyo caso habrán de ponderarse el conjunto de circunstancias concurrentes.

Por lo menos dos extremos nos parecen destacables. Primero la posibilidad de considerar vulneradora del derecho a la intimidad las grabaciones que tengan por objeto conversaciones sobre aspectos nucleares de la intimidad (punto b)), lo cual supone una relativización de la regla, que parecía asentada, de que la grabación de la conversación por parte de los interlocutores es (ya no) siempre lícita.

Segundo, que el engaño sobre los fines o la naturaleza de la conversación por parte de uno de los interlocutores o de un tercero pueden conllevar que la grabación resulte contraria al derecho a un proceso con todas las garantías. Esta consideración resulta especialmente relevante en el ámbito de las investigaciones internas. Según lo previsto en la Circular cabe deducir que no vale recurrir a **entrevistas o interrogatorios encubiertos o subrepticios**, grabados sin haber informado previamente al interlocutor.

- Aseguramiento de datos o informaciones contenidas en sistemas informáticos (punto 7.2)

La Circular aclara que la medida cautelar de aseguramiento de datos contenidos en sistemas informáticos no requiere de autorización judicial previa ni de una

motivación cualificada por su parte, dado que, con esta medida, no se afecta el derecho a la intimidad ni al secreto de las comunicaciones. El aseguramiento no implica un acceso a los contenidos. Simplemente garantiza su conservación.