*EL CIBERCONTROL DE LA PERSONA TRABAJADORA: DE FACULTAD EMPRESARIAL A OBLIGACIÓN IMPUESTA POR EL ESTADO.*

*Zaragoza. 9 de Mayo 2024*

*Juan Manuel San Cristóbal Villanueva.*

*Magistrado Director del Gabinete Técnico del Tribunal Supremo.*

 **ANEXO JURISPRUDENCIAL.**

 **1) Jurisprudencia del TEDH**

El Tribunal Europeo de Derechos Humanos ha tenido oportunidad de pronunciarse en múltiples ocasiones respecto del control tecnológico de los trabajadores. No puede olvidarse que el derecho a la intimidad se incardina en el art. 8 de la convención ( derecho a la vida personal y familiar) y en ella se incluyen por supuesto las comunicaciones de toda índole.[[1]](#footnote-1) En esta materia los pronunciamientos más destacables son los siguientes:

1.-**Sentencia del TEDH 5 de septiembre de 2017: Caso Barbulescu II contra Rumania.**

Este conocido caso es quizá el pronunciamiento más relevante en esta materia, por las circunstancias concurrentes, y porque supuso un radical cambio de criterio respecto del primer pronunciamiento del propio TEDH, que resultó corregido por la Gran Sala. Como es sabido, en este asunto se resuelve el caso de un trabajador (ingeniero de ventas) de una empresa privada que había instalado en su ordenador una aplicación de correo electrónico  *(Yahoo Messenger)* a petición del empresario, con el fin de recibir por esa vía preguntas de los clientes y poder responderlas.

La empresa había distribuido a los empleados una nota informativa en la que les alertaba de que verificaría el debido uso de los equipos, que no se debía navegar por Internet ni dedicar los equipos ni las aplicaciones informáticas a tareas que no eran estrictamente profesionales. Del mismo modo existían unas normas de uso de los ordenadores, pero en ella no se mencionaba la posibilidad de vigilar las comunicaciones realizadas a través de esos instrumentos. Sin embargo, el señor Barbulescu había utilizado esa cuenta de correo para su actividad privada y personal mediante la remisión y recepción de correos privados (correos a su novia y a su hermano).

Efectuada una monitorización de esos correos, la empresa lo detectó y el señor Barbulescu fue despedido. Como quiera que no obtuvo satisfacción de su derecho fundamental a la vida privada en los tribunales domésticos, acudió al TEDH, que en un primer momento no apreció tal vulneración. Sin embargo, la Gran Sala sí estimó tal vulneración del art. 8 del CEDH, y fijó lo que se ha dado en llamar el **“Test Barbulescu”,** de forma que habrá o no vulneración según la respuesta que se dé a las siguientes preguntas:

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

ii.) **Alcance de la supervisión y grado de intrusión:¿monitorización de flujo o del contenido de las comunicaciones? , ¿todas las comunicaciones o sólo parte de ellas?**.(¿Cuál fue el alcance de la supervisión realizada por el empleador y el grado de intrusión en la vida privada del empleado? A este respecto, debe distinguirse entre la monitorización del flujo de comunicaciones y de su contenido. También debe tenerse en cuenta si se han monitorizado todas las comunicaciones o sólo parte de ellas, así como la cuestión de si la monitorización fue limitada en el tiempo y el número de personas que tuvieron acceso a los resultados. Lo mismo se aplica a los límites espaciales de la monitorización).

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

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

v).-Qué **consecuencias ha tenido la intromisión inherente a ese control para el trabajado**r, y si la información obtenida se ha utilizado para alcanzar el objetivo declarado en la justificación de la medida adoptada.

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

**2) Sentencia del TEDH 9 de enero de 2018: Caso López Ribalda II y otros contra España.**

En este conocido caso, el TEDH abordó un supuesto de control videográfico del empleado, que, aunque desborda la faceta de la que nos estamos ocupando, tiene interés por cuanto se apoya en Barbulescu para llegar a semejante solución final. El caso, muy conocido, versaba sobre unas empleadas de una conocida empresa de supermercados en la que el empresario instaló unas cámaras de vigilancia ante la firme sospecha de que se estaban produciendo robos en las cajas del supermercado, lo que fue así comprobado, y las trabajadoras despedidas. Declarada la procedencia de los despidos por las diversas instancias domésticas, las trabajadoras acudieron al TEDH, postulando la vulneración de su derecho a la intimidad por considerar que no fueron previamente avisadas de la instalación de esas videocámaras, especialmente colocadas para vigilar las cajas, y distintas de las del resto de cámaras visibles colocadas por el local. Teniendo en cuenta que las actoras no fueron debidamente avisadas de ese control videográfico, así como que la LOPD señala en su art. 5 que se tiene derecho a ser informado previamente y de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, el TEDH en su primera sentencia de enero de 2018 entendió que había vulneración del art.8 de la Convención, entendiendo que no se había cumplido con ese principio de proporcionalidad por falta de previo aviso, por no comunicar el archivo de los datos y su posible finalidad disciplinaria, y por haber durado demasiado tiempo, pudiendo el empresario haber protegido sus intereses mediante un sistema menos intrusivo, o avisando con carácter general de la instalación de cámara ocultas en el local y dando la información exigida por la LOPD. Sin embargo, recurrida ante la Gran Sala, el TEDH en su segunda sentencia, de 2019, llega a la conclusión - modificando la previa decisión de la Sala ordinaria del TEDH de 2018- de que se había cumplido por los tribunales internos con ese principio de proporcionalidad pues llevaron a cabo un ejercicio de equilibrio detallado entre, por una parte, su derecho al respeto de su vida privada y, por otra, el interés del empleador en garantizar la protección de sus bienes y el buen funcionamiento de la empresa. Concluye que  los tribunales nacionales verificaron si la videovigilancia estaba justificada por una finalidad legítima y si las medidas adoptadas a tal efecto eran adecuadas y proporcionadas, observando en particular que la finalidad legítima perseguida por el empleador no podía alcanzarse con medidas menos intrusivas para los derechos de las demandantes. Y respecto de la no advertencia de instalación de esas nuevas cámaras, destaca el TEDH que si bien no se puede aceptar la proposición de que, en términos generales, la más mínima sospecha de apropiación indebida o de cualquier otro acto ilícito por parte de los empleados podría justificar la instalación de una videovigilancia encubierta por parte del empleador, la existencia de una sospecha razonable de que se ha cometido una falta grave y la magnitud de las pérdidas identificadas en el presente caso parecían una justificación de peso.

**3) Sentencia del TEDH 22 de febrero de 2018: Caso Libert contra Francia.**

En este supuesto, se aborda también el control del ordenador, pero ya no de un empleado de una empresa privada, sino de una Administración, una autoridad pública. En esta sentencia el TEDH señala que, si bien el empleador público puede abrir los archivos almacenados en el ordenador que se puso a disposición del empleado para el desempeño de sus funciones, **lo que no puede - salvo riesgo o acontecimiento especial- es abrir archivos identificados como personales** si no es en presencia de los empleados afectados o después de que hubieran sido oportunamente informados de que se iba a producir ese control. En el caso, el trabajador afectado no había identificado como personales ninguno de esos archivos, que fueron abiertos por su empresa. Se da la circunstancia de que había un archivo denominado “risas” que contenía videos y fotografías pornográficas, pero que el tribunal interno entendió que no estaba suficientemente identificado como “personal” o privado, visto que la capacidad de disco utilizada para tales fines era muy grande, lo que supuso que fuera perfectamente lógico que los tribunales internos aceptasen el control de tales archivos.

**B) Jurisprudencia del TC.**

El Tribunal Constitucional ha tenido oportunidad de pronunciarse también en diversas ocasiones sobre el control informático del empleado, y ello tanto antes como después de Barbulescu II. Los pronunciamientos más relevantes al respecto son los que se referirán a continuación, con la advertencia de que la doctrina del TC sobre la materia empezó a decantarse mediante el control del empleado por otros medios, como lo eran las grabaciones de video y audio, para pasar luego a las estrictamente informáticas.

Uno de los primeros casos de relevancia fue el de la **STC 98/2000, el caso del Casino La Toja**, bien conocido porque en él se abordó el supuesto de la posible vulneración del derecho a la intimidad de los trabajadores de la decisión del Casino de La Toja, S.A. consistente en instalar y utilizar unos aparatos de audición que permitían captar y grabar las conversaciones que tenían lugar en las secciones de caja y del juego de la ruleta francesa bajo el argumento de que esas grabaciones servían para completar los sistemas de seguridad y era útil para la empresa disponer de grabación del sonido en caso de tener que resolver eventuales reclamaciones de los clientes. El TC concluye que la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar. Por otro lado, la instalación de los micrófonos no fue efectuada como consecuencia de la detección de una quiebra en los sistemas de seguridad y control anteriormente establecidos, sino que, como se deducía del comunicado que la empresa remitió al Comité de empresa dando cuenta de la implantación del sistema de audición, se tomó dicha decisión para complementar los sistemas de seguridad ya existentes en el casino. Es decir, **no quedó acreditado que la instalación del sistema de captación y grabación de sonidos fuera indispensable para la seguridad y buen funcionamiento del casino.** Así las cosas, **el uso de un sistema que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores,** como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el art. 20.3 LET y **supone, en definitiva, una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE.**

Otro caso destacable es el que resolvió la **STC 186/2000 de 10 de julio**  **(caso** **Cajero del economato Ensidesa),** en el que se abordaba la constitucionalidad de la medida empresarial consistente en poner una cámara de videovigilancia instalada en el techo de la sección de ropa y calzado, en la zona de paso y tres cajas registradoras, y se concluye la concreción de tal medida por superar el test de proporcionalidad (necesidad, idoneidad y proporcionalidad estricta) ante las series sospechas de que el recurrente en amparo - que había sido despedido- había cometido graves irregularidades (sustrayendo diferentes cantidades ) en la zona de las cajas registradoras.

Ya en el concreto campo del control cibernético, es de reseñar la **STC 241/12, de 17 de diciembre,** en la que el TC destaca que indudablemente en al ámbito del control del empresario entra la **regulación del uso de los medios informáticos de su titularidad asignados al trabajador,** siendo a ello inherente la facultad de vigilar el correcto uso de esos elementos informáticos, siempre con respeto de los derechos fundamentales de los trabajadores. Se trataba de un trabajador que había instalado un programa de mensajería instantánea (Trillian) en un ordenador de uso compartido que le permitía mantener conversaciones con compañeros de trabajo y otras personas. La empresa al analizar su ordenador descubrió tal instalación y abrió decenas de mensajes sin su consentimiento ni conocimiento. Ello permitió concluir al TC que **no había perjuicio al derecho a la intimidad,** pues fue la propia trabajadora quien con su actuar ( instalar en el disco duro un programa en modo de acceso libre ) provocó que no se pudiera considerar vulnerado tal derecho fundamental ( art. 18.1 CE).

Respecto del derecho al secreto de las comunicaciones ( art. 18.3 CE), en el caso, tomando en cuenta que la decisión de la empresa se apoya en un hallazgo casual de otro empleado, y la intervención empresarial se limita a la comprobación de la instalación en el soporte informático de uso común, con la finalidad de constatar si había habido un incumplimiento por parte de las trabajadoras implicadas y su alcance, desarrollándose la actuación en un plazo razonable de dos meses, se concluyó que tampoco había vulneración.

Esta doctrina fue en cierto modo matizada por la **STC 29/2013 (Caso Universidad de Sevilla)** en la que se concede el amparo a un profesor que fue sancionado por **ausencias y faltas de puntualidad** que **se constataron a través de las cámaras** de seguridad instaladas a la entrada de la universidad. La imagen es una faceta de los datos de carácter personal (la sentencia se dicta una vez aprobada la Ley de protección de Datos) y su imagen se captó existiendo carteles de advertencia sobre la presencia de esas cámaras, pero no constaba la información previa, precisa y clara de su existencia y de su finalidad y posible utilización sancionadora.

Otra sentencia relevante es la del caso **STC 170/2013 de 7 de octubre ( caso Alcaliber)** que abordó el amparo solicitado por un empleado que fue objeto de despido disciplinario por transgresión de la buena fe, en el que, entre otros hechos, se le imputaba haber mantenido durante mucho tiempo una conducta de máxima deslealtad por haber **proporcionado indebidamente información confidencial de la empresa a personal de otra entidad mercantil,** sin haber pedido nunca autorización para ello y **utilizando en dicha transmisión medios que eran propiedad de la empresa —en concreto, teléfono móvil y correo electrónico-**. Se daba la circunstancia de que en esa empresa había una previsión en el convenio colectivo que tipifica como falta muy grave el uso indebido de los elementos informáticos y electrónicos puestos a disposición por el empresario, permitiendo solo el uso profesional, de tal suerte que no podía hablarse de una expectativa legítima de confidencialidad en las comunicaciones efectuadas por esos medios. Y además había una sospecha del comportamiento irregular del trabajador. Se daba también el dato relevante de que la única forma de saber si se cumplían las normas pactadas era acceder al contenido de los correos, no bastando con comprobar los destinatarios con los que se había mantenido la correspondencia electrónica, siendo además que ninguno de los correos abiertos contenía información personal. No hubo , en opinión del TC, ni vulneración de la intimidad ni del secreto de las comunicaciones porque se superaba el test de proporcionalidad.

También de importancia es la **STC 39/2016 (Caso Bershka):** la empresa había detectado desajustes en las cuentas de las cajas registradoras y decidió instalar unas cámaras enfocadas a esa zona, junto con una señal en el escaparate indicando de manera general en el local la existencia de videovigilancia, con lo que consiguió grabar a algunos trabajadores apropiándose de dinero de la caja . Ello permitió al TC responder que no hubo violación del art 18.4 ( protección de datos) pues se supera el test de proporcionalidad.

Es conveniente recordar la doctrina contenida en la **STC 61/2021** (**Caso Amadeus y control ordenador)**. Se trataba del despido de una trabajadora de una empresa tecnológica, por, entre otros incumplimientos alegados, la falta de tiempo para desempeñar sus tareas, haber dedicado en torno a un 30 por 100 de su jornada laboral a labores profesionales, empleando el 70 por 100 de la jornada restante a solventar cuestiones del ámbito de su esfera personal o, sencillamente, a no realizar labor alguna, lo que se descubrió cuando , tras una sospecha, se procedió en secreto a monitorizar su ordenador. El juzgado no admitió la prueba de monitorización del ordenador por considerar que se tradujo en el conocimiento del contenido de mensajes de correo electrónico de carácter personal y dirigidos a sus familiares, y declaró la existencia de vulneración del derecho fundamental al secreto de las comunicaciones y con ello la nulidad del despido. Por el TSJ se confirmó tal apreciación sobre la nulidad de la prueba, pero negó que eso generase la nulidad del despido, sino sólo la ilicitud de la prueba y la improcedencia del despido en base a los demás incumplimientos no acreditados. El TC concluyó que la ilicitud de la prueba no puede generar *per se* la nulidad del despido. En efecto , la cuestión se centra en determinar si en el caso de que se acredite en el procedimiento laboral que una fuente de prueba utilizada para justificar el despido se ha obtenido vulnerando derechos o libertades fundamentales, **dicha ilicitud debe proyectarse sobre la calificación del despido, de tal manera que este debe ser declarado nulo –planteamiento defendido en términos generales por la demandante de amparo y con carácter más limitado por el Ministerio Fiscal– o sí por el contrario la ilicitud de la prueba únicamente produce como efecto su expulsión del acervo probatorio** por aplicación del art. 90.2 LJS –y también del art. 11.1 LOPJ– del que resulta que «no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas», sin que dicha exclusión probatoria pueda afectar a la calificación del despido, que será declarado improcedente o procedente en función de que existan o no otras pruebas, planteamiento este defendido en la sentencia impugnada y apoyado por la entidad empleadora.

El tema es de legalidad ordinaria, por lo que no es terreno propio del TC, pero aun así señala que la negativa a la nulidad en tales casos no merece ser calificada de arbitraria o de manifiestamente irrazonable. No hay pues vulneración de la tutela judicial efectiva, aunque en el caso se devuelven las actuaciones para que se resuelva sobre la indemnización solicitada por el afectado.

Por último, puede citarse la **STC 119/2022, de 29 de septiembre (Caso Saltoki).**

En ella se descarta la vulneración del derecho de protección de datos y de intimidad del trabajador despedido que había sido grabado cometiendo un acto ilícito -entregar unos productos propiedad de la empresa demandada a un tercero que le abona un dinero en metálico del que se apropia, absteniéndose de entregar albarán de entrega ni recibo de pago alguno, - porque “las cámaras no estaban instaladas en lugares de descanso, ocio o de carácter reservado, en los que existiera una expectativa razonable de privacidad, sino que estaban instaladas en zonas de trabajo abiertas a la atención al público. En segundo lugar, las cámaras no estaban instaladas de forma subrepticia, sino que estaban ubicadas en lugares visibles, tanto para los trabajadores del establecimiento como para el público en general. En tercer lugar, las cámaras no fueron utilizadas con carácter generalizado o indefinido, o para realizar una investigación de carácter prospectivo, sino para verificar la posible existencia de una conducta irregular detectada el día anterior. Por lo tanto, el grado de intromisión en la esfera de la intimidad del trabajador (art. 18.1 CE), en términos de espacio y tiempo, no puede considerarse como desequilibrado frente a los derechos e intereses de la empresa en la detección y sanción de las conductas atentatorias contra la buena fe contractual, en el marco del ejercicio de los derechos a la propiedad privada y a la libertad de empresa, reconocidos en los arts. 33 y 38 CE, respectivamente”.

**C) Jurisprudencia del TS**

Probablemente fue la **STS de 26/09/2007 – R. 966/2006 -(Caso CORUÑESA)** el primer pronunciamiento del alto tribunal al respecto del control del ordenador por parte del empresario, que tuvo un enorme eco doctrinal y social y marcó la senda inicial a seguir.

Como se recordará, en ella se abordaba el caso del despido de un trabajador que había visitado páginas de Internet poco seguras, sufriendo ese ordenador la infección o contaminación de varios virus. La empresa, tras conocer el funcionamiento defectuoso de ese ordenador, y en presencia del administrador de la empresa detectó la existencia en la carpeta de archivos temporales de antiguos accesos a páginas pornográficas que se almacenaron en un dispositivo de USB que se entregó a un notario, retirando el ordenador de la empresa para su reparación. El TS concluye que ese acceso no es irregular ni inconstitucional y que no le es extensible las garantías que el ET contempla para la taquilla (durante el trabajo, con representante de los trabajadores y presencia del afectado), pues la taquilla está destinada a guardar los objetos personales, mientras el ordenador es un instrumento de trabajo, recordando doctrina anterior ( STS 5 /12/2033 ) en la que se afirmaba que en materia de telemarketing la empresa podría grabar y monitorizar las llamadas para corregir defectos de técnica comercial y controlar el trabajo. Respecto a la garantía de intimidad con el ordenador, el TS señaló que es **reconocible una tolerancia social y empresarial** al uso personal de elementos patrimoniales de la empresa (teléfono y ordenador) que crea una expectativa general de confidencialidad en esos usos. Así dice el TS lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de **prohibiciones absolutas o parciales-** e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

Otro pronunciamiento antiguo, pero de relevancia, lo configura **la STS 08/03/2011 ( R. 1826/2010 (Caso Font Salem. Las 5.566 visitas) .** En ella **l**a cuestión planteada se ofrece desde la perspectiva de la **licitud de la prueba obtenida**: para la empresa recurrente, el acceso al ordenador fue perfectamente lícito y sin vulneración de derecho fundamental alguno. Sin embargo como señala el Tribunal, la prueba de esas interminables visitas a páginas de Internet había sido obtenida por la empresa a partir de una auditoría interna en las redes de información con el objetivo de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios informáticos puestos a disposición de los empleados, y **no consta que de acuerdo con las exigencias de la buena fe, la empresa hubiera establecido previamente algún tipo de reglas para el uso de dichos medios especificando la existencia de prohibiciones absolutas o parciales ni tampoco que se hubiera informado a los trabajadores** de que se iba a proceder al control y la forma en que dicho control iba a llevarse a cabo, lo que lleva al TS a concluir que la prueba no fue lícitamente obtenida.

Curiosamente, si bien las dos sentencias citadas transitan en su argumentación bajo el paraguas de la aceptación de un uso razonable de los medios tecnológicos, sin embargo la **STS 06/10/2011 ( -R.4053/2010, Caso Annaligia, Programa espía)** para un supuesto en el que constaba una prohibición expresa del uso personal del ordenador perfectamente conocida por las trabajadoras, y sin embargo éstas procedieron a un uso particular del ordenador visitando diversas páginas de Internet, tanto de compras como reserva de billetes, búsqueda de empleo etc., acaba concluyendo la inexistencia de una expectativa de intimidad. El comportamiento irregular fue comprobado mediante un programa espía que simplemente captaba las imágenes de pantalla que se iban visionando y de cuya existencia no sabían las afectadas. El tribunal concluyó que, si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo.

No podemos seguir nuestro análisis cronológico sin referirnos a la **STS 8 /2 /2018 -Rcud 1121/ 2015 ( Caso Inditex. control ordenador),** un supuesto en el que el TSJ mantuvo la procedencia del despido por transgresión de la buena fe de un vendedor de la empresa que aceptó que un proveedor le pagase un coche, aunque, no obstante, afirmó que eran nulas las pruebas ilícitamente obtenidas a través del control electrónico de su correo. El TS atribuyó plena validez procesal a la prueba del examen del correo existente en ordenador del trabajador. Avala su decisión lo siguiente:

a) el examen del ordenador es acordado tras el hallazgo casual de fotocopias de transferencias de un proveedor a favor del actor, lo que excluye la doctrina del fruto del árbol emponzoñado,

b) la previa prohibición de usar el ordenador de la empresa para fines particulares hace que no haya derecho para hacerlo en condiciones que impongan respeto a la intimidad, el ponderado examen del correo electrónico utilizando el servidor de la empresa y parámetros de búsqueda informática orientados a limitar la invasión de la intimidad, evidencia que se han respetado los requisitos exigidos por la jurisprudencia constitucional y se han superado los juicios de idoneidad, necesidad y proporcionalidad, criterios coincidentes con la STEDH de 5/9/17.

Dignas de mención son también las sentencias dictadas en el **Caso IFEMA (STS 21/ 7 /2021 -Rcud 4877/ 2018 y STS 25 / 1/ 2022 -Rcud 4468/2018).**

En esta cadena de recursos se cuestionó la corrección jurídica de la inadmisión de una prueba de videovigilancia, porque en opinión de los órganos jurisdiccionales inferiores no se había dado debida cuenta a los trabajadores de la posible finalidad controladora del desarrollo del trabajo de la instalación de cámaras. En estos casos los respectivos trabajadores prestaban servicios como vigilantes de seguridad en un acceso de vehículos de Ifema, dándose la circunstancia de que el director de seguridad del recinto comunicó y reiteró a Securitas que se habían detectado graves irregularidades en el cumplimiento de las instrucciones referidas a los controles (requisas) de seguridad en vehículos. Se procedió al visionado de las imágenes y se comprobó que un total de quince vigilantes registraban controles que no constaba que se hubieran realizado. Se les notificó su despido disciplinario y en el proceso judicial la empresa trató de aportar como prueba la grabación de las cámaras del sistema de videovigilancia que fue inadmitida. El TS recuerda la doctrina de la STEDH Ribalda I fue rectificada y corregida por la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), así como que la STC 39/2016, 3 de marzo de 2016, sentó la doctrina de que, **cuando el trabajador conoce que se ha instalado un sistema de control por videovigilancia no es obligado especificar «la finalidad exacta que se le ha asignado a ese control»**. La prueba de la reproducción de lo grabado por las cámaras de videovigilancia era, así, una medida justificada, idónea, necesaria y proporcionada al fin perseguido, por lo que satisfacía las exigencias de proporcionalidad que imponen la jurisprudencia constitucional y del TEDH.

Un supuesto semejante, es el que abordó la **STS 13/10/21 - Rcud 3715/18. (Caso Autobús)**.En ella el Juzgado de lo Social declaró el despido procedente al admitir la prueba de videovigilancia aportada por la empresa para justificar el despido disciplinario del trabajador (conductor de bus urbano público) y comprobar los incumplimientos acontecidos con anterioridad a la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. La Sala del TSJ estimó el recurso de suplicación del trabajador y lo declaró nulo. El TS confirma ese pronunciamiento y declara correcta la admisión de la prueba de videovigilancia aportada por la empresa para justificar el despido disciplinario, casa, anula y devuelve actuaciones al TSJ para que con libertad de criterio entre a resolver los restantes motivos del recurso de suplicación. **Los trabajadores habían sido informados de la existencia de las cámaras de grabación, bien señalizadas**. Aplica la Doctrina TEDH y TC (conocimiento, no necesario consentimiento, idoneidad, adecuación, justificación, necesidad y proporcionalidad).

Cabe mencionar aún tres pronunciamientos más para terminar esta relación de sentencias relevantes en materia de control tecnológico del trabajador.

Por un lado **la STS 15/9/2020- Rcud 528/2018 (Caso GPS),** un supuesto relevante en el que el TS casa y anula la de suplicación que declaró la nulidad del despido disciplinario de la trabajadora, a la que la empresa le facilitó un vehículo para el desempeño de su actividad en jornada laboral, vehículo que disponía de un dispositivo GPS, lo que se documentó por escrito entre la empresa y la trabajadora, y que fue despedida por haber utilizado el vehículo durante el fin de semana previo a la incapacidad temporal que padeció y durante ésta. Argumentó que debe equilibrarse el respeto a la protección de datos y la eventual invasión de la intimidad del trabajador, equilibrio que se consigue cuando existe una expectativa de intimidad del trabajador bien porque existen disposiciones o reglas expresas o un uso social de tolerancia. Atendiendo a ello, **considera que la instalación del GPS por la empresa tiene la finalidad de garantizar la seguridad y coordinación del trabajo, sin que en la carta de despido se refleje ninguna circunstancia personal de la trabajadora, sino movimientos en tiempos no justificados**, lo que además era conocido por la trabajadora, por lo que procede la declaración de procedencia del despido por no vulneración de sus derechos fundamentales.

En segundo lugar, es digno de mención el supuesto resuelto en la **STS 8/3/2022 -R. 130/2019 ( Caso BBVA) ,** que declara la improcedencia del despido de una empleada respecto de la que la entidad bancaria para la que prestaba sus servicios utilizó su conocimiento de los datos de la cuenta corriente de la trabajadora para configurar prueba de los posibles incumplimientos laborales realizados por la empleada que era titular de la referida cuenta. Se trataba, en definitiva, de considerar lícita o no, en relación a los derechos fundamentales a la intimidad y a la protección de datos, la prueba consistente en la utilización, sin su autorización, de los datos de la cuenta corriente que la trabajadora tenía abierta en la entidad empleadora. Y se concluye que el despido es nulo, siendo los datos de la cuenta corriente de la trabajadora datos de carácter personal y que fueron usados sin autorización ni información previa de la trabajadora, para fines distintos de los que podrían derivarse de una legítima finalidad, anudada al contrato mercantil sobre cuenta corriente bancaria existente entre las partes.

Y en tercer lugar, el caso de la **STS 22/7/2022 -R. 701/2021 (Caso videovigilancia encubierta de empleada de hogar),** un supuesto en el que una familia instaló una cámara oculta en la habitación de la demandada ( que sufría una tetraplejia traumática) para comprobar si las sospechas de hurto por parte de la empleado de hogar eran ciertas, una vez que descubrieron que una trampilla del armario de la habitación de la enferma que simulaba unos cajones y escondía una caja fuerte, estaba mal colocada, y dentro faltaba una suma importante de dinero (30.000 euros). La grabación confirmó tales sospechas, pero obviamente, ni se puso distintivo alguno en el domicilio de advertencia de la instalación de cámaras de vigilancia, ni se advirtió a la empleada. La Sala tras recordar que si bien la Ley de protección de Datos 3/18 en su art. 89.1 impone la obligación de advertencia expresa, clara y concisa de la existencia de cámaras de grabación y tratamiento de esas imágenes, en su párrafo segundo recoge la excepción : «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores … 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» en referencia al cartel genérico de zona videovigilada, sin necesidad de notificación expresa.

Así pues, dice la sentencia que comentamos, en determinadas circunstancias, la STEDH 17 de octubre de 2019 (López Ribalda II), admite que la empresa no advierta al trabajador de la existencia ni del emplazamiento de determinadas cámaras de videovigilancia, de manera que esa ausencia de información no ha de conducir necesariamente a la no toma en consideración de la prueba de videovigilancia que sustenta la sanción al trabajador y acredita el incumplimiento y su autoría

Sentado lo anterior resuelve que:

 1) **La videovigilancia era una medida justificada e idónea para el fin perseguido,** ya que estamos ante a) una justificación seria: el alcance de lo denunciado como cantidad sustraída en el domicilio familiar en el que prestaba servicios la empleada (30.000 euros y otras monedas y billetes antiguos sustraídos de una cámara fuerte, así como joyas); b) La cámara únicamente enfocaba al armario en el que estaba instalada la caja fuerte, sin que lo hiciera sobre ningún otro punto de la habitación ni del hogar familiar y c) es relevante la gran vulnerabilidad de la empleadora.

2) En cuanto al **posible incumplimiento de la legislación de protección de datos** tiene otras consecuencias y otras posibles protecciones - denuncia ante la Agencia de protección de Datos- que no se agotan en el debate sobre la validez de la prueba de videovigilancia en un proceso por despido por incumplimiento normativa de protección de datos.

3) **La imposibilidad de que se considere en el proceso de despido la prueba de videovigilancia, que es a la conclusión a la que llega la sentencia recurrida, deja inerme a la empleadora, especialmente vulnerable**, para poder acreditar el grave incumplimiento acaecido y su autoría. No es fácil imaginar - dice la sentencia- con qué otra prueba podría acreditarse dichos incumplimientos y la autoría, que la empleadora está obligada a probar en el juicio por despido.

Por todo ello, concurría la imperativa protección de importantes intereses, que pueden ser no sólo "públicos", sino también "privados", protección que "puede justificar la ausencia de “información previa". Y termina la Sala insistiendo en que “estamos examinando un supuesto excepcional y singular, de manera que sólo excepcionalmente y si se dan circunstancias similares a las aquí concurrentes se podrá prescindir del distintivo informativo mencionado.”

Octubre 2023

J*UAN MANUEL SAN CRISTÓBAL VILLANUEVA.*

*Magistrado Director del Gabinete Técnico del Tribunal Supremo*

1. En el precepto citado se incluye el derecho al respeto de la “correspondencia”, en el sentido del artículo 8, apartado 1, que tiene como objetivo proteger la confidencialidad de las comunicaciones en numerosas situaciones diferentes. Esta noción abarca, por supuesto, el correo privado o profesional (Niemietz c. Alemania, § 32 in fine), las conversaciones telefónicas entre los miembros de una misma familia (Margareta y Roger Andersson c. Suecia, § 72), o con terceros (Lüdi c. Suiza, §§ 38-39;Klass y otros c. Allemagne, §§ 21 y 41;Malone c. Reino Unido, § 64), las llamadas telefónicas desde locales privados o profesionales (Amann c. Suiza [GS], § 44;Halford c. Reino Unido, §§ 44-46;Copland c. Reino Unido, § 41;Kopp c. Suiza, § 50) y desde una cárcel (Petrov c. Bulgarie, § 51) y la “intercepción” de información relacionada con tales conversaciones (fecha, duración, números marcados) (P.G. y J.H. c. Reino Unido, § 42).409. Las tecnologías, por supuesto, también entran en el ámbito de aplicación del artículo 8 y, en particular, los mensajes electrónicos (correos electrónicos) (Copland c. Reino Unido, § 41;Bărbulescu c. Rumanía[GS], § 72), el uso de internet (Copland c. Reino Unido, §§ 41-42), los datos almacenados en servidores informáticos (Wieser y Bicos Beteiligungen GmbH c. Austria, § 45), incluidos los discos duros (Petri Sallinen y otros c. Finlandia, § 71) y los disquetes informáticos (Iliya Stefanov c. Bulgaria, § 42). 410. También afecta a las más antiguas y en muchos casos superadas formas de comunicaciones electrónicas como los télex(Christie c. Reino Unido, Decisión de la Comisión), los mensajes por medio de buscapersonas (Taylor-Sabori c. Reino Unido), así como las emisiones por radio privada (X e Y c. Bélgica, Decisión de la Comisión), sin incluir aquellas en una frecuencia pública y, por lo tanto, accesibles para otros (B.C. c. Suiza, Decisión de la Comisión). [↑](#footnote-ref-1)