www.upo.es/revistas/index.php/lex_social/index
julio - diciembre 2020
Vol. 10 núm. 2 / 2020
Revista jurídica de los Derechos Sociales
Lex Social

CONTROL EMPRESARIAL DEL USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL DESDE LA PERSPECTIVA DEL DERECHO A LA PROTECCIÓN DE DATOS Y A LA INTIMIDAD

BUSINESS CONTROL OF THE USE OF DIGITAL DEVICES IN THE LABOR FIELD FROM THE PERSPECTIVE OF THE RIGHT TO DATA PROTECTION AND PRIVACY

MERCEDES LÓPEZ BALAGUER
FRANCISCO RAMOS MORAGUES

Departamento de Derecho del Trabajo y de la Seguridad Social[*]
Universidad de Valencia

Artículo recibido el 2 de diciembre de 2019
Artículo aceptado el 18 de diciembre de 2019

DOI: https://doi.org/10.46661/lexsocial.5075

RESUMEN

Los avances tecnológicos no sólo han permitido una evolución en los procesos productivos o en la forma organizativa y de trabajar de las empresas, sino que también han posibilitado que éstas escojan nuevas formas y métodos de supervisión de la actividad laboral más invasivos, que, en ocasiones, entran en colisión con los derechos fundamentales de los trabajadores, entre ellos, el derecho a la protección de datos y el derecho a la intimidad. La vigente Ley de Protección de Datos destina algunos preceptos a regular el control y acceso por parte de la empresa a los dispositivos digitales facilitados al trabajador. El presente trabajo analiza estos preceptos y los rasgos más destacados de su régimen jurídico.

[*] Profesora Titular de Universidad y Profesor Contratado Doctor. Este trabajo se inscribe en el marco del Sub-proyecto DER2017-83488-C4-3-R del Ministerio de Ciencia, Innovación y Universidades "Los derechos fundamentales del trabajo subordinado en la era digital" del que forma parte, como investigadora, la profesora Mercedes López Balaguer.

PALABRAS CLAVE: Protección de datos, control empresarial, intimidad.

ABSTRACT

Technological advances have not only allowed an evolution in the production processes or in the organizational and working form of companies, but have also enabled them to choose new, more invasive forms and methods of supervising work activity, which, on occasions , collide with the fundamental rights of workers, including the right to data protection and the right to privacy. The current Data Protection Law allocates some precepts to regulate the control and access by the company to the digital devices provided to the worker. The present work analyzes these precepts and the most outstanding features of its legal regime.

KEYWORDS: Data Protection, employer control, privacy.

SUMARIO

1. A modo de introducción.

El intercambio de información y de datos personales en favor de terceros forma parte de nuestra cotidianidad. Comportamientos rutinarios en la vida de las personas como el uso de las redes sociales, navegar por internet o realizar transacciones *on line* a través del móvil se traducen, por cuanto aquí interesa, en una transmisión, a escala mundial y de forma inmediata, de una ingente cantidad de datos, muchos de los cuales, son de carácter personal. No admite discusión las enormes ventajas que traen consigo los avances

tecnológicos y, fruto de estos, los nuevos servicios digitales puestos a disposición de la ciudadanía; sin embargo, esas mismas ventajas pueden convertirse en un problema de cara a garantizar la protección de determinados derechos fundamentales, señaladamente, del derecho a la protección de datos, de la privacidad e intimidad de las personas.

Es verdad que la necesidad de garantizar una tutela adecuada de estos derechos no es una cuestión novedosa; sino que ha ocupado la atención de doctrina y jurisprudencia desde tiempo atrás. Ahora bien, aun siendo esto cierto, no lo es menos que la sociedad está experimentando en los últimos tiempos una verdadera revolución digital, que está transformando profundamente la forma que tenemos de vivir, trabajar y relacionarnos[1] y que, por ende, hacen que aquella necesidad de tutela a la que aludíamos anteriormente adquiera una nueva dimensión[2].

Centrándonos en el tratamiento de datos y su protección, el ejemplo más claro de la nueva dimensión que adquiere, hoy por hoy, esta materia, la podemos observar de forma clara en la aparición de nuevas aplicaciones informáticas, nuevas herramientas digitales y, particularmente, en el recurso a las tecnologías *Big Data*. En efecto, este tipo de tecnologías -*Big Data*- permiten a través de algoritmos la obtención de una enorme cantidad de datos personales, de información sobre nosotros mismos que se registra como una suerte de "huella" que vamos dejando al realizar actividades en la Red. *A priori* se trata de datos aislados, desconectados, que no guardan relación unos con otros; no obstante, su tratamiento por medio estas tecnologías posibilita ofrecer un perfil de las personas y obtener un conocimiento sobre nuestros gustos, hábitos, intereses, etc. Por ello, puede afirmarse que el recurso a las tecnologías de *Big Data* se erige como un elemento estratégico fundamental para mejorar los procesos de negocios, incrementando los beneficios y analizando los eventuales riesgos existentes[3]

Como señalábamos anteriormente, el incremento exponencial de las posibilidades de transmisión de información que nos ofrece el actual entorno digital y las múltiples herramientas que lo integran, tiene una desventaja evidente; y es que, paralelamente también han aumentado los riesgos de obtener información sin nuestro consentimiento y, aún peor, de que se utilice indebidamente, con las consecuencias que ello puede tener para nuestra seguridad y privacidad. Asumiendo que al progreso tecnológico ni puede ni es razonable ponerle trabas; los esfuerzos han de concentrarse en eliminar o reducir a la mínima expresión las consecuencias negativas que derivan de aquél; y, desde luego, una de las formas más eficaces para cumplir ese objetivo es configurando una adecuada

[1] *Vid*., el documento elaborado por la CEOE, rubricado "Plan de digitalización 2020. La digitalización de la sociedad española", 2016, pág. 11. El texto completo del documento se encuentra disponible en: http://contenidos.ceoe.es/CEOE/var/pool/pdf/publications_docs-file-334-plan-digital-2020-la-digitalizacion-de-la-sociedad-espanola.pdf [Consulta realizada el 1 de noviembre de 2019].

[2] GARCÍA MURCIA, Joaquín. y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", Revista Española de Derecho del Trabajo, núm. 216, 2019 [Artículo consultado en la versión digital].

[3] Se refiere a esta cuestión, URRUTIA SAGARDÍA, Eneko. "Importancia estratégica del *Big Data*", *Actualidad Jurídica Aranzadi*, núm. 935, 2017 [Artículo consultado en la versión digital].

protección de la privacidad de las personas, configurando instrumentos normativos idóneos.

Por supuesto, el ámbito laboral no es ajeno a las consideraciones que acabamos de señalar. En efecto, al igual que acontece con los particulares, en las relaciones laborales el tráfico de información es una constante. Se manejan datos personales del trabajador como su nombre y apellidos, su nacionalidad, dirección, titulación, conocimientos, capacidad laboral, número de teléfono móvil, entre otros. Del mismo modo, el desarrollo de las herramientas tecnológicas se proyecta también sobre la privacidad de los trabajadores desde una triple perspectiva[4]: en primer lugar, permiten a las empresas un mayor acceso, tanto cuantitativa como cualitativamente, a informaciones personales de los trabajadores. En segundo lugar, como consecuencia de la generalización de los recursos técnicos, se han difuminado las fronteras entre la vida laboral y la vida privada[5]. En tercer lugar, los nuevos sistemas tecnológicos posibilitan que la empresa pueda ejercer un control mucho más incisivo del cumplimiento de las obligaciones laborales por parte de los trabajadores.

Es precisamente el recurso a las nuevas tecnologías como herramientas de control de la actividad laboral lo que ha propiciado mayores conflictos en sede judicial. Conflictividad que, en parte, responde a la ausencia de una normativa específica que regulase la facultad de control empresarial[6]. Hasta fechas relativamente recientes, la única previsión a este respecto era el art. 20 ET, en cuya virtud: "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

Esta situación de déficit normativo ha propiciado la creación de una elaborada doctrina jurisprudencial, tanto del Tribunal Supremo como del Tribunal Constitucional -interpretada y, en ocasiones, modificada por la doctrina del Tribunal Europeo de Derechos Humanos- de la que es posible extraer las reglas y parámetros interpretativos a tener en cuenta a la hora de valorar si existe un adecuado equilibrio entre el control de la actividad laboral y el respeto al derecho a la intimidad y a la protección de datos del trabajador.

[4] GOERLICH PESET, Jose María., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico", en AA.VV. *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pp. 124-125.

[5] Como bien ha destacado un sector de la doctrina, las nuevas tecnologías facilitan que la prestación de servicios se extienda más allá de la jornada y del lugar de trabajo instaurándose una suerte de cultura laboral basada en la "disponibilidad permanente". *Vid*., GOÑI SEIN, Jose Luís., "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016, *Revista de Derecho Social*, núm. 78, 2017, pág. 19.

[6] Se trata de una de las críticas que desde tiempo atrás viene formulando la doctrina científica, por todos: DE LOS COBOS ORIHUEL, Francisco. y GARCÍA RUBIO, Amparo. "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de los Derechos Humanos", en *Revista Española de Derecho del Trabajo*, núm. 196, 2017. [Artículo consultado en su versión digital].

En este estado de las cosas, el panorama descrito ha cambiado, en parte, con la aprobación de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPD). Ello es debido, de un lado, a que la citada norma ha incluido determinados preceptos que regulan de forma específica el uso de los dispositivos digitales en el ámbito laboral; imponiendo, luego volveremos sobre ello, límites explícitos al ejercicio del poder de control empresarial; y, de otro, a la introducción de un nuevo art. 20 *bis* al ET rubricado: "derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión".

En este contexto, el objeto de estudio del presente trabajo se va a centrar en el análisis del uso de los dispositivos digitales facilitados al trabajador y su eventual control por parte de la empresa conforme al nuevo marco normativo establecido por la LOPD; señaladamente, se analizarán los arts. 87, 89 y 90 de la norma antedicha. Asimismo, teniendo en cuenta que, tal y como se ha dicho, la utilización de las nuevas tecnologías como herramientas de control ha generado -y sigue haciéndolo- una enorme litigiosidad en el ámbito jurídico-laboral, parece conveniente que al hilo del análisis del derecho sustantivo se incluyan algunas referencias en orden a la licitud de la prueba en el proceso laboral en el marco del derecho fundamental del trabajador a la protección de datos y a la intimidad. Téngase en cuenta que las nuevas tecnologías además de ser una herramienta de control, también son el medio de prueba utilizado por la empresa para acreditar el incumplimiento laboral que legitima el ejercicio del poder disciplinario. A mayor abundamiento, debe recordarse que, tal y como indica el art. 90.2 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, la inadmisión de la prueba será la consecuencia jurídica aplicable al origen u obtención de la prueba mediante procedimientos que impliquen violación de derechos fundamentales o libertades públicas.

Vaya por delante, en fin, que además del análisis normativo hemos incorporado a nuestro estudio los principales criterios interpretativos manejados por la jurisprudencia, nacional e internacional, a la hora de resolver los conflictos jurídicos que se han ido suscitando; y ello con el propósito último de valorar en qué medida los cambios normativos acontecidos pueden suponer un cambio en las tesis jurisprudenciales hasta ahora predominantes.

2. Protección de datos e intimidad: derechos con sustantividad propia.

Antes de adentrarnos en lo que constituye el núcleo duro del presente trabajo es importante hacerlo a partir de una premisa previa y fundamental, a saber: el derecho a la intimidad y el derecho a la protección de datos son derechos que presentan, cada uno de ellos, una sustantividad propia. En otras palabras, entre los datos personales y la intimidad no existe una coincidencia absoluta[7]. Por tanto, en la práctica, unos hechos puedan ser constitutivos de una vulneración del derecho a la protección de datos y no del derecho a la intimidad; y, viceversa. Pero vayamos paso a paso.

[7] GARCÍA MURCIA, Joaquín. y RODRÍGUEZ CARDO, Iván. Antonio., "La protección de los datos personales en el ámbito del trabajo: una aproximación desde…", *op. cit*. p. 36.

Para empezar, cuando se habla de "datos personales" se está haciendo referencia a aquellos que sirven para identificar a una persona. Es lo cierto que, generalmente, son datos estrechamente relacionados con la privacidad de las personas y que, obvio es decirlo, pueden estar vinculados con su intimidad. Es el caso, por ejemplo, de una fotografía, del nombre y apellidos de una persona o del número de documento nacional de identidad. Sin embargo, el concepto de intimidad es más restringido; de hecho, hay datos que siendo personales no pertenecen al ámbito de la intimidad de una persona. Desde esta perspectiva, se ha dicho que la intimidad protege la esfera más reservada de las personas mientras que la privacidad abarca "[…] facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca, pero que, enlazadas entre sí, arrojan un retrato de la personalidad del individuo que este tiene derecho a mantener reservado"[8].

La sustantividad propia que presenta el derecho a la protección de datos frente a la intimidad se desprende del propio reconocimiento constitucional del derecho. En este sentido, repárese en que el art. 18.4 de la Constitución Española (en adelante, CE) reconoce este derecho de forma autónoma; esto es, independiente del derecho al honor, *a la intimidad* y a la propia imagen (art. 18.1 CE). El que tengan un tratamiento diferenciado evidencia que el objeto y contenido de ambos derechos fundamentales es diferente y, como consecuencia de ello, es imprescindible la articulación de instrumentos normativos específicos que hagan posible la dispensa de una tutela adecuada dependiendo del derecho de que se trate.

En todo caso, el carácter independiente del derecho a la protección de datos frente a la intimidad no es algo novedoso. Desde tiempo atrás la jurisprudencia del Tribunal Constitucional ha defendido la tesis de que este derecho no es una mera especificación del derecho a la intimidad. Especialmente ilustrativa es, en este sentido, su conocida sentencia de 30 de noviembre del 2000, motivada por un recurso de inconstitucionalidad presentado frente a determinados incisos de la extinta Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal. Tesis que, por lo demás, ha sido acogida con posterioridad por la jurisprudencia laboral[9].

El Alto Tribunal diferenciará en la sentencia citada el objeto de protección en ambos derechos y su contenido, concluyendo que se trata de derechos fundamentales con sustantividad propia. Sin pretensión de exhaustividad, el TC comenzará su argumentación afirmando que el derecho a la intimidad se muestra insuficiente para proteger el tráfico de datos personales. Conclusión que responde a la propia voluntad del constituyente. Razona el máximo interprete de la constitución que aquél, sabedor de los riesgos que podría entrañar el uso de la informática, decidió incluir un apartado cuarto en el art. 18 como "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio). Prueba de esta voluntad de configurar un

[8] MERCADER UGUINA, Jesús Rafael., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Ed. Francis Lefebvre. Claves Prácticas, Madrid, 2019, p. 23.
[9] STS (Orden Social) de 7 de febrero de 2018 (rec. 78/2017).

tratamiento autónomo a la protección de datos no sólo es su plasmación final en el texto constitucional sino el propio debate seguido en sede parlamentaria, en el que si bien se pudo cuestionar inicialmente la necesidad del apartado 4 del art. 18 habida cuenta de que ya se reconocían los derechos a la intimidad y al honor, finalmente se consideró que aquellos derechos, en atención a sus contenidos, "[…] no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada"; razón por la cual, era necesario un ámbito de protección específico y, por ende, más idóneo, que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el art. 18.1 CE.

Partiendo de esta idea, el Tribunal proseguirá en su argumentación diferenciando entre intimidad y protección de datos. De entrada, se afirmará que "la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona". Así pues, si bien ambos derechos comparten el fin último de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, su objeto es distinto. Mientras el derecho a la intimidad extiende su garantía a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, esto es, los datos íntimos de la persona; el derecho fundamental a la protección de datos, en cambio, amplía aquella garantía constitucional, al extenderla a aquellos datos que "[…] sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado". Consecuentemente, cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, quedan dentro del objeto de protección del derecho previsto en el art. 18.4 CE. Se incluirían, también "datos personales públicos", que, pese a ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. En definitiva, se afirma que "[…] los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

Finalmente, el TC fijará su atención en el contenido del derecho. También en este punto se observarán singularidades. El derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido; por el contrario, el contenido del derecho fundamental a la protección de datos consiste "[…] en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Tales poderes de disposición y control sobre los datos personales requieren como complemento

indispensable, indica el TC, "[…] la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".

Si descendemos del plano jurisprudencial al normativo, es posible identificar disposiciones normativas que asumen ese carácter autónomo del derecho a la protección de datos. De entrada, la Carta de los Derechos Fundamentales de la Unión Europea, en su art. 8.1, afirma que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". Igualmente, el Reglamento 2016/679 en su art. 1.2 establece que esta norma "protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales". A mayor abundamiento, en su art. 88, el Reglamento de 2016 prevé, precisamente para el ámbito de las relaciones laborales, que los diferentes Estados miembros puedan establecer normas "más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral".

Así y todo, es difícil sostener estrictamente una afirmación en estos términos si acudimos a la regulación específica que hace para el ámbito laboral la LOPD 2108; pues, paradójicamente, y, a nuestro entender, criticablemente, no se ha incorporado de manera expresa la referencia al derecho de protección de datos. Basta con acudir a los preceptos destinados al ámbito laboral en relación con el control empresarial, para comprobar que se refieren exclusivamente al derecho a la intimidad en relación con el uso de los dispositivos y la videovigilancia; la única referencia al derecho de protección de datos es en relación con la geolocalización. Es más, el nuevo art. 20 *bis* ET, introducido por la comentada Ley Orgánica, reconoce "el derecho a la intimidad" de los trabajadores "en el uso" y "frente al uso" de los dispositivos digitales. En definitiva, no se ha querido incorporar al texto estatutario el derecho de protección de datos como derecho fundamental, a pesar de su autonomía respecto al derecho a la intimidad.

Sea como fuere, se insiste una vez más, en línea con el parecer manifestado por la jurisprudencia constitucional (*vid. supra*) y por la doctrina científica que se ha ocupado de esta cuestión[10], el derecho de protección de datos es un derecho que muchas veces abarca y alcanza al derecho a la intimidad, pero son categorías diferentes y, esa diferencia,

[10] MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* p. 24, que considera que la clave del diferente alcance de ambos derechos puede encontrarse en la regulación de la CDFUE, ya que la consagración en la CDFUE de la protección de datos como derecho autónomo (art. 8) se ha hecho de modo separado y diferente del derecho al respecto a la vida privada y familiar (art. 7); en parecido sentido, GARCÍA MURCIA, Joaquín y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde…", *op. cit.* p. 36, señalan que, tanto por su enunciado como por el contenido que efectivamente se les atribuye en el correspondiente pasaje legal, no siempre se trata de prácticas o decisiones relacionadas con la obtención o el uso de datos personales. Más bien se trata de supuestos en los que pueden o suelen quedar afectados otros bienes del trabajador, como su intimidad o su esfera personal o privada, al menos de manera principal o más inmediata. Y, añaden estos autores, que estos preceptos de la LOPD parecen restar alguna capacidad de impacto al derecho a la protección de datos porque la invocación de ese derecho había permitido conceder una tutela cualitativamente más intensa o perfeccionada que los derechos tradicionales, gracias a la disociación que hacía la jurisprudencia entre consentimiento e información.

implica que los mismos hechos, como decíamos, pueden ser vulneración de uno de los derechos y no del otro.

3. El ejercicio de los derechos fundamentales en el marco de una relación laboral a la luz de la doctrina constitucional clásica: criterios generales.

La Constitución Española de 1978 destina su Título I al reconocimiento de los "Derechos y deberes fundamentales" y, dentro de este, proclama en sus arts. 14 a 29 los denominados como derechos fundamentales. Se trata de derechos inherentes a las personas, esto es, derechos y libertades cuya titularidad se predica de todo ciudadano por el mero hecho de serlo y que gozan, por mor de la posición de preeminencia que ocupan en el ordenamiento jurídico, de un status singular de protección. A nadie escapa que este grupo de derechos constitucionales también pueden ejercitarse por los trabajadores en el marco de un contrato laboral, conformando así lo que la doctrina iuslaboralista ha venido a calificar como "derechos de la persona del trabajador"[11] o "derechos fundamentales inespecíficos"[12].

El ejercicio de estos derechos y su posible modulación al hacerse valer en el ámbito de las relaciones laborales no es una materia novedosa por lo que a su análisis se refiere. Antes al contrario, se trata de un tema recurrente para los estudiosos de la rama social del derecho que ha despertado, desde siempre, un gran interés y atención por parte de la doctrina científica; atención e interés que si acudimos a los repertorios de jurisprudencia y estudios doctrinales más recientes, no parece haber desaparecido con el paso del tiempo. Especialmente cuando fruto de los avances tecnológicos, el debate se centra en si existe un justo equilibrio entre el uso de las legítimas facultades empresariales de control y la posible vulneración de los derechos y libertades de los trabajadores a la hora de llevar a cabo dicha supervisión.

Antes de centrarnos en la nueva regulación que establece la LOPD 2018, parece conveniente efectuar alguna alusión, siquiera sea brevemente, a cuáles han sido las líneas maestras que desde tiempo atrás viene estableciendo el Tribunal Constitucional español (en adelante, TC) en punto al alcance, límites e interacciones entre derechos fundamentales y relaciones de trabajo. Repárese en que el ordenamiento jurídico español, a salvo de algún precepto concreto, no contempla un cuerpo normativo que discipline esta cuestión, razón por la cual, ha sido el TC y la jurisprudencia quienes han asumido un papel protagonista en la determinación de las reglas y criterios necesarios para ponderar la influencia recíproca entre las dos variables mencionadas[13]; contribuyendo, en líneas

[11] VALDÉS DAL-RÉ, Fernando, "Poderes del empresario y derechos de la persona del trabajador", *Relaciones Laborales*, 1990, núm. 1, pp. 277-294.

[12] PALOMEQUE LÓPEZ, Manuel Carlos, "Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos", en AA.VV. (Dir. SEMPERE NAVARRO, Antonio Vicente), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003, p. 229.

[13] RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, Miguel. "La integración de los derechos fundamentales en el contrato de trabajo", en AA.VV. (Dir. Sempere Navarro, A.V.), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003, p. 209.

generales, a crear un clima favorable al respeto de los derechos en el interior de las empresas[14].

Como punto de partida, interesa significar que uno de los rasgos característicos de la relación que existe entre el contrato de trabajo y los derechos fundamentales es la presencia de una limitación mutua o recíproca entre ambos elementos[15], de manera que, por un lado, el ejercicio de tales derechos en el ámbito laboral aparece sujeto a importantes restricciones cuyo origen reside en las obligaciones dimanantes del propio contrato de trabajo, en el principio de buena fe contractual y en el poder de dirección del empresario; y, a sensu contrario, los derechos fundamentales del trabajador juegan como un límite al contrato de trabajo en un doble sentido[16]: primero, impidiendo que aquél pueda contener cláusulas que sean contrarias al ejercicio de los mismos; y, segundo, obligando a que el desempeño de las facultades inherentes al poder empresarial sean respetuosas con su ejercicio. Como consecuencia de esta limitación mutua, será necesario proceder en cada caso a una adecuada ponderación que respete la valoración constitucional del derecho fundamental en juego y las obligaciones laborales que pueden modularlos[17].

Sobre la base de esta idea inicial, el TC parte de una premisa básica sobradamente conocida por todos, según la cual, "la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano…". Y es que, "ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad ni la libertad de Empresa que establece el art. 38 del Texto Constitucional legitima el que quienes prestan servicios en aquélla por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional"[18]. Dicho en otras palabras, los derechos fundamentales que tiene el trabajador en su condición de ciudadano no desaparecen por el mero hecho de que éstos se desplieguen en el ámbito laboral[19].

No obstante lo anterior, el reconocimiento de la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral no implica desconocer que tales derechos no presentan un carácter absoluto o ilimitado, sino que su ejercicio "debe enmarcarse en unas determinadas pautas de comportamiento […] no siendo discutible que la existencia de una relación contractual entre trabajador y empresario genera un complejo de derechos y obligaciones recíprocas que condiciona el ejercicio de

[14] VALDÉS DAL-RÉ, Fernando., "Poderes del empresario y derechos de la persona del trabajador", op. cit., p. 292.
[15] DEL REY GUANTER, Salvador. "Derechos fundamentales de la persona y contrato de trabajo: notas para una teoría general", *Relaciones Laborales*, 1995, núm. 1, p.
[16] Idem., op. cit., p. 205.
[17] Por todas, STC de 12 de enero de 1998 (RTC 1998/1).
[18] STC de 19 de julio de 1985 (Rec. 788/1984), cuya doctrina se reitera posteriormente, entre muchas otras, en las SSTC de 21 de enero de 1988 (Rec. 1221/1986); y de 17 de julio de 1989 (Rec. 987/1987).
[19] GARCÍA-PERROTE ESCARTÍN, Ignacio. "Ley, convenio colectivo, contrato de trabajo y derechos fundamentales del trabajador", *Revista de Derecho Social*, núm. 4, 1998, p. 46.

tales derechos fundamentales de modo que manifestaciones del mismo que en otro contexto pudieran ser legítimas no tienen por qué serlo necesariamente dentro del ámbito de dicha relación"[20].

La cuestión determinante, pues, no estriba en si estos derechos despliegan su vigencia en el contrato de trabajo, lo que no admite discusión a la vista de la doctrina jurisprudencial expuesta, sino más bien, determinar cuál es el alcance que se le deba atribuir a tales derechos[21]. El TC asume esta importante labor teniendo en cuenta dos premisas fundamentales[22]: de un lado, la posición de preeminencia que ocupan los derechos fundamentales en nuestro ordenamiento jurídico, que los sitúa por encima del ejercicio de otro tipo de derechos que no gozan de idéntica protección; y, de otro lado, que en el supuesto de existir un conflicto entre derechos fundamentales, ha de buscarse una solución que en la medida de lo posible garantice el ejercicio de todos ellos, o, en todo caso, que no se vean algunos de ellos lesionados de forma irremediable.

Sin perder de vista esta doble consideración, la doctrina constitucional ha recalcado en infinidad de ocasiones que cualquier restricción del ejercicio de los derechos fundamentales en la relación laboral no sólo ha de resultar acorde al principio de buena fe contractual que caracteriza al contrato de trabajo, sino que, además, la actuación empresarial deberá respetar tanto el principio de indispensabilidad como el de proporcionalidad. El primero de ellos supone que no es suficiente la sola afirmación del interés empresarial existente para considerar las limitaciones al ejercicio de un derecho fundamental como ajustadas a derecho. La posición prevalente tantas veces aludida que tienen los derechos fundamentales en nuestro ordenamiento jurídico se traduce en que "[…] los requerimientos organizativos de la empresa que pudieran llegar a ser aptos para restringir el ejercicio de aquéllos –al margen de los conectados de forma necesaria con el objeto mismo del contrato– deben venir especialmente cualificados por razones de necesidad, de tal suerte que se hace preciso acreditar por parte de quien pretende aquel efecto que no es posible de otra forma alcanzar el legítimo objetivo perseguido, porque no existe medio razonable para lograr una adecuación entre el interés del trabajador y el de la organización en que se integra"[23].

La aplicación del criterio de indispensabilidad expuesto ha de conjugarse necesariamente con el segundo de los principios mencionados, esto es, el principio de proporcionalidad, consistente básicamente en que la medida restrictiva de derechos fundamentales deberá superar lo que se ha venido a calificar por la doctrina como el "triple juicio"[24]. Es decir,

[20] STC de 15 de diciembre de 1983 (Rec. de amparo núm. 69/1983).

[21] PRADOS DE REYES, Francisco Javier, "Contrato y relación de trabajo", en AA.VV., *Veinte años de jurisprudencia laboral y social del Tribunal Constitucional*, Tecnos, Madrid, 2001, p. 181.

[22] ARIAS DOMÍNGUEZ, Ángel y RUBIO SÁNCHEZ, Francisco, *El derecho de los trabajadores a la intimidad*, Aranzadi, Cizur Menor (Navarra), 2006, p. 40.

[23] STC de 11 de abril de 1994 (Rec. 797/1990).

[24] GARCÍA-PERROTE ESCARTÍN, Ignacio.; Y MERCADER UGUINA, Jesús Rafael, "Conflicto y ponderación de los derechos fundamentales de contenido laboral", en AA.VV. (Dir. Sempere navarro, A.V, A.V), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003, p. 257.

será imprescindible que dicha medida sea idónea para conseguir el objetivo propuesto –juicio de idoneidad-; que no exista la posibilidad de adoptar otra medida menos gravosa para el trabajador que permita alcanzar tal propósito con igual eficacia –juicio de necesidad–; y, por último, que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto –juicio de proporcionalidad en sentido estricto-[25]. Sólo cuando concurran estos requisitos, lo que obligará a realizar un análisis de cada caso concreto, el contrato de trabajo podrá limitar en los términos expuestos el ejercicio de un derecho fundamental por parte del trabajador.

4. El poder de control empresarial a la luz de las nuevas previsiones específicas contenidas en la LOPD: arts. 87, 89 y 90.

Como es bien sabido, el poder de dirección del empresario tiene su encaje constitucional en el art. 38, encargado de proclamar el derecho a la libertad de empresa en el marco de la economía de mercado. En palabras del propio TC, la libertad de empresa entraña "[…] el reconocimiento a los particulares de una libertad de decisión no sólo para crear empresas y, por tanto, para actuar en el mercado, sino también para establecer los propios objetivos de la empresa y planificar su actividad en atención a sus recursos y a las condiciones del propio mercado"[26]. Para hacer efectivo ese derecho y garantizar que el titular de la empresa pueda adoptar las decisiones estratégicas y organizativas que determinarán el futuro de la misma, el ordenamiento jurídico laboral le atribuye una serie de facultades organizativas, directivas, de supervisión y vigilancia y disciplinarias que conforman todas ellas los denominados como "poderes empresariales". Este poder, en cualquiera de sus manifestaciones, no presenta un carácter absoluto, sino que se sujeta a importantes limitaciones tanto subjetivas (referidas a quién lo ejerce: el empresario o la persona en quien este delegue) como objetivas, encontrándose, en esta última categoría, el respeto a la dignidad del trabajador y a sus derechos y libertades fundamentales.

De las diferentes facultades que se acaban de enumerar interesa referirnos en este foro a la posibilidad de vigilar la actividad laboral y, de manera más concreta, a la utilización por la empresa de medios audiovisuales o técnicos como, por ejemplo, los sistemas de videovigilancia o los sistemas que permiten controlar el uso del ordenador, Internet o el correo electrónico profesional por los trabajadores. Los avances tecnológicos no sólo han permitido una evolución en los procesos productivos o en la forma organizativa y de trabajar de las empresas sino que también han posibilitado que éstas escojan nuevas formas y métodos de supervisión de la actividad laboral más invasivos que, en ocasiones,

[25] Sobre el principio de proporcionalidad y su alcance pueden consultarse, entre muchas otras, las SSTC de 8 de mayo de 1995 (Rec. 1693/1992); de 28 de marzo de 1996 (Cuestiones de inconstitucionalidad núm. 1125/1995, 2736/1995 y 961/1994); de 17 de febrero de 1998 (Rec. 3694/1994); de 10 de julio de 2000 (Rec. 2662/1997) de 7 de mayo de 2012 (Rec. 8640/2010); de 7 de noviembre de 2013 (Rec. núm. 2907/2011); y de 3 de marzo de 2016 (Rec. 7222/2013).
STC de 8 de julio de 1993 (Rec. 418/1987 y 421/1987 núm. 1902/1991y1904/1991).

[26] STC de 8 de julio de 1993 (Rec. 418/1987 y 421/1987 núm. 1902/1991y1904/1991).

entran en colisión con los derechos fundamentales de los trabajadores, entre ellos, por descontado, los de protección de datos e intimidad; lo que se ha traducido en una enorme litigiosidad en torno a la validez determinados medios de control y sobre su uso empresarial.

A ello ha contribuido, sin duda, la parca regulación legal de esta facultad empresarial. Como decíamos en otra parte de este trabajo, hasta fechas relativamente recientes, salvo alguna previsión más específica relativa a los registros del trabajador (art. 18 ET) y sobre la exigencia de reconocimientos médicos (art. 20.4 ET); el único precepto legal que de manera general se refería -y sigue haciéndolo- a este poder era el art. 20 ET, que de una forma genérica permite al empresario poner en marcha las medidas que considere convenientes para vigilar y controlar el cumplimiento de la actividad laboral. Con lo cual, aquél goza de un amplio margen para designar y utilizar el concreto medio de control con el que verificar el cumplimiento de las obligaciones laborales del trabajador, sin perjuicio del límite general referido a *"*la consideración debida a su dignidad*"*; límite que, por su conexión con la "dignidad de la persona" que encabeza el Título I de la CE se relaciona con el necesario respeto a los derechos fundamentales, en particular, los vinculados con la intimidad[27]. La valoración de si el medio de control escogido por la empresa y el uso que se hace del mismo se ajusta o no a derecho dependerá, una vez más, del caso concreto; y, además, la solución al conflicto planteado deberá producirse aplicando la doctrina general sobre el ejercicio de los derechos fundamentales en el contrato de trabajo.

La situación descrita, por lo que al marco normativo aplicable se refiere, se ha visto afectada por la aprobación del Reglamento 2016/679/UE, de 27 de abril, de Protección de Datos (REPD); y, sobre todo, por su concreción en el derecho interno a través de la Ley Orgánica 3/2018 de homónimo título. Y es que, en aplicación de lo dispuesto en el art. 88 del REPD[28], la LOPD ha regulado los procedimientos de control en el uso o frente al uso de dispositivos digitales en los que se puede ver afectado el derecho de protección de datos y el derecho a la intimidad –art. 20 bis ET y arts. 87 a 89 LOPD-.

Así pues, los Tribunales para poder decidir el ejercicio de la facultad de control empresaria ha sido o no respetuosa con el derecho fundamental de protección de datos y con el derecho de intimidad, deberán comprobar si se han cumplido las exigencias que recoge la norma sustantiva. Vaya por delante, en cualquier caso, que esta tarea no será fácil dado que, como se ha considerado, en opinión que compartimos, la nueva regulación

[27] GOERLICH PESET, José María, "Poderes del Empresario", en AA.VV. (Coord. CAMPS RUÍZ, Luís. y RAMÍREZ MARTÍNEZ, Juan Manuel), *Derecho del Trabajo*, Tirant lo Blanch, Valencia, 2016, p. 441.
[28] El precepto comunitario habilita a los Estados miembros para que establezcan, a través de normas legislativas o convenios colectivos, disposiciones más específicas de protección, en relación, particularmente, con la "contratación de personal, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados y clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de extinción de la relación laboral"

"aporta más sombras que luces al desarrollo de los derechos digitales en el ámbito laboral, en la medida en que genera importantes dudas interpretativas"[29].

Sentado lo anterior, pasamos a analizar estas exigencias siguiendo el orden previsto por la propia Ley. Es decir, en primer lugar, nos detendremos en el control de los dispositivos digitales puestos a disposición del trabajador; en segundo lugar, en el control del cumplimiento de las obligaciones laborales mediante videovigilancia y grabación de sonidos; y, por último, en el control mediante sistemas de geolocalización. En este análisis seguiremos un esquema idéntico para los tres supuestos, recordando primero, muy brevemente, el nuevo marco normativo y pasando después a estudiar tanto la interpretación que los Tribunales están empezando a hacer de la normativa actual como la doctrina jurisprudencial y del TC que a lo largo de los años ha venido valorando la licitud de la prueba en base a la normativa anterior. Respecto de esta doctrina anterior se deberá comprobar además si, con la nueva normativa, sigue siendo aplicable o ha quedado superada en algún caso.

4.1. El control del trabajador mediante el acceso a los dispositivos digitales puestos a su disposición por la empresa.

El art. 87 LOPD regula el derecho a la intimidad en el uso de los dispositivos digitales y lo hace de manera «progresiva» en el marco de la relación laboral, esto es, tras reconocer el derecho a la intimidad del trabajador y el derecho al control de la empresa, apunta cuál debe ser el espacio legal para la confluencia de ambos derechos y, en consecuencia, el espacio de licitud de la prueba obtenida por el empresario tras el control del dispositivo que el trabajador utiliza en su actividad profesional del día a día.

En efecto, de entrada, el precepto legal no aporta nada nuevo al reconocer que los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. Y es que, tal derecho ya se contemplaba en la anterior Ley de protección de datos amen de haber sido reconocido tanto por la doctrina del TS como del TC o del TEDH. Asimismo, repárese en que el uso de los dispositivos digitales hace referencia a la actividad desempeñada por el trabajador en el entorno digital (correo electrónico, uso de internet, mensajería digital, uso de aplicaciones…) y es por ello que, aunque el art. 20 bis y el 87.1 LOPD se refieren al derecho de intimidad, otros derechos pueden estar también en juego (por ejemplo, el derecho al secreto de las comunicaciones)[30].

[29] SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *IusLabor,* 3/2018, [versión digital], p. 218.

[30] Ya lo señaló el TS (social) en su sentencia de 26 de septiembre de 2007, rec. 966/2006: "En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada «navegación» por Internet y en el acceso a determinados archivos personales del ordenador". Sobre esta cuestión, DESDENTADO BONETE, A. y DESDENTADO DAROCA, E., "La segunda sentencia del

A continuación, reconoce al empresario la facultad de acceder al contenido de los dispositivos digitales puestos a disposición de los trabajadores, pero siempre y cuando dicho acceso responda a uno de estos dos objetivos: controlar el cumplimiento de las obligaciones laborales o garantizar la integridad del dispositivo. De este modo, se incorpora a la norma la "justificación legítima" que tradicionalmente los Tribunales han venido exigiendo al empresario a la hora de acceder a los dispositivos digitales y que impide que aquél se produzca de manera injustificada, indiscriminada o constante.

A este respecto, el TEDH en la conocida sentencia *Barbulescu II*, de 5 de septiembre de 2017, vino a señalar que "el empleador tiene un legítimo interés en asegurar el buen funcionamiento de su empresa, aplicando medidas que le permitan verificar que sus empleados cumplen con sus deberes profesionales de manera adecuada y con la celeridad requerida". En el ámbito nacional, ya la STS de 26 de septiembre de 2007, dejaba clara la idea de que los dispositivos digitales son propiedad de la empresa y que ésta se los proporciona al trabajador para que sean empleados en el cumplimiento de la prestación laboral, "por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario como precisa el artículo 20.3 ET".

En suma, a través de los dos primeros apartados del art.87 se está asumiendo la doctrina clásica del TC en la que se reconoce[31]:

Primero, que "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

Segundo, que "el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE) y reconocido expresamente en el art. 20 LET, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales" pero "que el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador".

Tercero y, como corolario de lo anterior, que es necesario que se preserve "el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito –modulado por el contrato, pero en todo caso subsistente– de su libertad constitucional pues, dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación sólo deberá producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del

Tribunal Europeo de Derechos Humanos en el caso *Barbulescu* y sus consecuencias sobre el control del uso laboral del ordenador", *Información Laboral*, 1/2018, BIB 2018\6059 [versión digital].

[31] Por todas, STC 123/1992, de 28 de septiembre; STC 134/1994, de 9 de mayo; STC 6/1998, de 13 de enero; y STC 186/2000, de 10 de julio.

trabajador y, muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE, teniendo siempre presente el principio de proporcionalidad".

Si el primer apartado del art. 87 reconoce el derecho a la intimidad del trabajador; y, el segundo, el derecho del empresario a controlar la actividad laboral accediendo al uso de los medios digitales facilitados; el apartado tercero se referirá al procedimiento que deberá seguir aquél para que su control legítimo sea además respetuoso con el derecho fundamental a la intimidad del trabajador.

A nuestro modo de ver, el legislador, a través del art. 87.3 LOPD, ha venido a configurar un doble y gradual estándar de intimidad; cuya graduación depende de la prohibición o admisión del uso privado de los dispositivos digitales que los empresarios deben comunicar de manera previa a los trabajadores tras decidirlo con la participación de los representantes de los trabajadores[32].

El cumplimiento de este deber de información, que debe ser considerado contenido esencial del derecho a la intimidad del trabajador[33], implica que de antemano el trabajador sabe que nos podemos encontrar dos escenarios:

Por un lado, que, según los criterios facilitados por la empresa, el uso se limite exclusivamente al ámbito profesional. En tal caso, el empresario "[…] deberá respetar los estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente".

Por el otro, que, conforme a dichos criterios empresariales, esté permitido el uso de los dispositivos digitales con fines privados. En estos supuestos, el empresario "[…] deberá especificar de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados".

En el primer escenario de prohibición total del uso privado, que es hoy posible desde una interpretación literal de la norma[34], nos moveríamos en lo que legislador ha denominado *estándar mínimo* de protección de la intimidad. Y, en el segundo, estaríamos ante en lo que podríamos denominar como *estándar reforzado* de protección de la intimidad.

En base a lo anterior, desde el plano procesal, la licitud de la prueba que se obtenga a partir de ese control dependerá de que el estándar aplicable se haya respetado en todo caso y, en consecuencia, lo que hoy por hoy no plantea duda alguna es que el derecho a

[32] Con esta exigencia, asume la LOPD una de las recomendaciones del importante *Dictamen 2/2017 del GT 29 sobre el tratamiento de datos en el trabajo* que recomienda que, en todos los casos, una muestra representativa de trabajadores participe en la evaluación de la necesidad del control, así como en la lógica y accesibilidad de la política. [Dictamen consultado en versión digital Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm].

[33] SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 219.

[34] En este sentido, SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 219; y, MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…,* op. cit., p. 132. Para ambos autores la dicción literal del art. 87 LOPD lleva a interpretar que es posible que el empresario limite absolutamente el uso privado de los dispositivos digitales.

la intimidad es un límite al control empresarial de los dispositivos digitales tanto en el primer supuesto como en el segundo.

En este sentido, creemos[35] que con la nueva LOPD no sería posible admitir como lícita una prueba tras el control del dispositivo afirmando 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" (STS de 6 de octubre de 2011[36]). Ni tampoco consideramos que sea posible sostener con el nuevo marco normativo que ofrece la LOPD que es lícita la prueba obtenida con el control del dispositivo porque "no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe" (STC 170/2013, de 7 de octubre).

En el primer ejemplo, la ilicitud de la prueba obtenida sería la consecuencia aplicable al incumplimiento del actual art. 87.3 LOPD cuando expresamente reconoce que el estándar mínimo de intimidad sigue siendo exigible aun en casos de prohibición absoluta del uso privado del dispositivo. En el segundo, la ilicitud de la prueba obtenida sería consecuencia de la inexistencia de información suficiente a los trabajadores porque, tal y como señala el mencionado artículo en su último párrafo, estos han de ser informados de los criterios de utilización y la referencia en el convenio al carácter leve de la falta no parece que pueda cumplir con esta exigencia.

A nuestro juicio, cabe entender que en materia de obtención de prueba a través del control de los dispositivos digitales se puede considerar que resultan hoy aplicables como criterios interpretativos del nuevo art. 87 LOPD, en primer lugar, la doctrina jurisprudencial asentada desde la sentencia de 26 de septiembre 2007, que se sintetiza en tres puntos utilizando los principios clásicos de la doctrina constitucional sobre

[35] En el mismo sentido, para SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 220, que considera que "la expectativa de intimidad y secreto de las comunicaciones sigue vigente, aunque exista una prohibición empresarial expresa y absoluta del uso personal de los dispositivos digitales, salvo que el empleador informe con la debida antelación de la naturaleza, tipo y alcance del control, así como del grado de intrusión en la vida privada social (la que se desarrolla en el lugar de trabajo)".

[36] rec. 4053/2010. Hay que tener en cuenta que esta sentencia matizó de manera muy importante la doctrina de 2007, admitiendo, como señala MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* p. 133, el control sin la información previa del mismo asumiendo "que no hay garantía de intimidad cuando existe prohibición absoluta de usos personales, aunque no se hayan formulado advertencias de control".

proporcionalidad, necesidad e idoneidad: a) el trabajador tiene derecho al respeto a su intimidad en el uso de los dispositivos digitales; b) la empresa de acuerdo con las exigencias de buena fe debe 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"; c) si el dispositivo se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que se ha vulnerado el derecho a la intimidad. Y, en segundo lugar, desde la perspectiva de la doctrina del TEDH, debemos acudir obviamente a la sentencia *Barbulescu II* a la que ya nos hemos referido y que se resume en el denominado *test* de siete ítems[37]: a) Información previa y clara a los trabajadores de las medidas de control; b) Nivel de control: extensión temporal y material; c) Justificación legítima; d) Alcance comparativo del control: la fórmula más respetuosa con la vida privada; e) Uso de la información obtenida con el control; f) Trasparencia en el acceso al dispositivo[38].

En este sentido, la STS de 8 de febrero de 2018, rec. 1121/2015, resulta especialmente interesante para el tema que nos ocupa porque, aunque no aplica lógicamente la LOPD de 2018, resuelve un supuesto en el que se cuestiona precisamente la licitud de la prueba obtenida tras el control de un ordenador de la empresa –de hecho, la empresa recurre la sentencia dictada en suplicación, aunque el despido fue declarado procedente por admisión de otras pruebas[39]-, que previamente había informado sobre el uso exclusivamente profesional del mismo. En el caso planteado se acredita la existencia de normativa empresarial sobre los sistemas de información y sobre la política de seguridad de la información que limita el uso de los ordenadores de la empresa a los estrictos fines laborales y que prohíbe su utilización para cuestiones personales. Esta información aparece en la pantalla del ordenador cada vez que los trabajadores acceden al mismo y expresamente incluye una referencia a que "el acceso lo es para fines estrictamente

[37] Así lo han denominado TERRADILLOS ORMAETXEA, Edurne., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social*, n. 80, 2017, pp.139-162; y, BLASCO JOVER, Carolina., "Trabajadores "transparentes": la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados (I)", *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*, Volumen 6, núm. 3, julio-septiembre de 2018, p. 40.

[38] Además consideramos, en línea con lo que señala MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* pp. 137-138, que es importante que, a la hora de valorar el procedimiento de control de los dispositivos desde la perspectiva del derecho a la intimidad, se utilice también el Dictamen 2/2017 del GT 29, al que ya hemos hecho alusión, porque puede resultar en el plano práctico un guía muy interesante como orientación para implementar procedimientos de control válidos desde el parámetro de la proporcionalidad. En este Dictamen se encuentran ejemplos de tecnologías de control de los dispositivos no invasivas o mínimamente invasivas que las empresas deben utilizar en la medida de lo posible.

[39] Y el TS entiende que ha lugar al recurso precisamente por "la posible exigencia de responsabilidades de todo orden por una actuación de la empresa que la sentencia recurrida ha calificado atentatoria a derechos fundamentales del trabajador".

profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de su empleados, respetando en todo caso la legislación laboral y convencional sobre la materia y garantizando la dignidad e intimidad del empleado". Por otra parte, en relación con la justificación legitima del control en el asunto planteado el examen del ordenador utilizado por el trabajador se realiza tras el «hallazgo casual» de una documentación de la que cabía inferir un incumplimiento del deber de buena fe del trabajo expresamente prohibido en el Código de Conducta de la empresa. Y, finalmente, en relación con el alcance del control se constata que el examen del correo electrónico se limita al de la cuenta de correo corporativo y se lleva a cabo con restricciones tanto temporales como de contenido mediante el acceso al servidor alojado en las propias instalaciones de la empresa.

A nuestro juicio, el supuesto planteado y resuelto en esta sentencia podría considerarse como un ejemplo de un sistema de control que se ajustaría a lo previsto en el actual art. 87.3 LOPD en el caso de aplicación de un protocolo de exclusivo uso profesional del dispositivo. Entendemos esto porque, aunque no compartimos algunos de los argumentos expuestos en la fundamentación jurídica de esta sentencia –en particular, los referidos a la doctrina del TS y del TC que consideramos superada por la actual regulación-, de acuerdo con la descripción de las circunstancias en las que se lleva a cabo el control, parece que se cumplen en el procedimiento de obtención de la prueba los requerimientos de la actual normativa de protección de datos en relación con los criterios de interpretación de la misma que aquí sostenemos. Así, en primer lugar, se cumple con el requisito de la información previa sobre la limitación estricta al uso profesional del dispositivo, detallándose en la información los criterios de uso. En segundo lugar, se advierte de que la empresa podrá proceder al control del mismo y se informa sobre que este se desarrollará en el marco del derecho a la intimidad. Y, en tercer lugar, se constata que en efecto ese control se realiza del modo menos invasivo posible por lo que a la afectación del derecho fundamental se refiere[40].

En el segundo de los escenarios, esto es, en el supuesto de que el sistema aplicable en la empresa permita el uso privado de los dispositivos digitales (art. 87.3.2ºpárr.) ya hemos visto que la información deberá ser mucho más detallada, incluyendo en todo caso la delimitación del derecho de los trabajadores al uso privado y el detalle de las garantías que los mismos tienen respecto del mismo. En este caso, como decíamos antes, parece que el legislador ha considerado necesario reforzar el estándar de intimidad del trabajador, dado que es obvio que, habilitado el uso personal de la herramienta digital de trabajo,

[40] En el mismo sentido parece entenderlo SERRANO OLIVARES, Raquel., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 222. En contra de esta interpretación BLASCO JOVER, Carolina, "Trabajadores "transparentes": la facultad fiscalizadora…", *op. cit.,* p. 47, sostiene una posición crítica considerando que la resolución del TEDH realiza el análisis del triple juicio de una forma más rigurosa y exigente que los Tribunales nacionales, que ya no podrán legitimar la medida fiscalizadora empresarial, sobre la existencia de una política de uso de los medios informáticos, sino que deberán revisar si existe la misma, a continuación, ponderar si aquélla supera el triple juicio antes indicado y, finalmente, si se ofrecieron las debidas garantías al trabajador.

habrá que reconocer y diseñar expresamente una frontera entre el espacio personal y profesional de uso. Y ese delimitado espacio va a resultar esencial a la hora de valorar si el procedimiento de control del dispositivo necesario para la obtención de la prueba ha sido o no respetuoso con el derecho a la intimidad del trabajador.

En relación con ello, un ejemplo práctico y que puede resultar muy útil a las empresas y a los representantes de los trabajadores a la hora de elaborar el protocolo de uso de los dispositivos digitales que permita el uso privado es el que ofrece la importante STEDH de 22 de febrero de 2018, asunto *Libert contra Francia*. En este asunto, el Tribunal de Estrasburgo decidió que no es contraria al art. 8 CEDH la normativa francesa que permite que cuando se han negociado protocolos de uso de los dispositivos digitales que permiten el uso privado, la empresa pueda acceder y abrir los archivos profesionales que estén almacenados en el disco duro de los ordenadores de la empresa cuando no estén identificados correctamente como privados. Concretamente, en este caso, el Acuerdo colectivo negociado con los representantes de los trabajadores había previsto que "excepto riesgo o acontecimiento especial", la empresa no podría acceder a los archivos identificados como "Privados". Pues bien, en el concreto supuesto de hecho, los archivos a los que la empresa accede estaban identificados de otro modo –con la palabra "risas" y en unidad "D:/datos personales"- y tras acceder a los mismos la empresa constata sin duda la transgresión de la buena fe contractual –entre otras cosas el trabajador había utilizado una parte importante de la capacidad de su ordenador profesional para almacenar 1.562 archivos representando un volumen de 787 Mb-. Con estos datos, el TEDH considera que, aún en un supuesto en el que la empresa había consentido el uso privado de los medios digitales profesionales, el incumplimiento de los requisitos –siquiera formales- fijados para ese uso privado, puede justificar el acceso de la empresa a los mismos y la imposición de la correspondiente sanción no puede ser considerada contraria al art. 8 CEDH.

4.2. El control del trabajador mediante sistemas de videovigilancia.

El art. 89 LOPD se ocupa de regular la videovigilancia como sistema de control empresarial. En este sentido, en relación con el derecho fundamental a la intimidad de los trabajadores, es el precepto que establece el marco legal para que la obtención de pruebas mediante esta técnica de vigilancia sea respetuosa con ellos.

En la misma línea que la seguida para los dispositivos digitales, el precepto legal reconoce, en primer término, el derecho de los empresarios a tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control "siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo". A partir de este reconocimiento, también en el supuesto de videovigilancia es posible distinguir diversos escenarios, cada uno de los cuales, contarán con un nivel de protección.

El primer escenario es que los empleadores hayan informado con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso,

a sus representantes, acerca de esta medida –se trata de lo que podemos denominar «cámaras informadas»-.

El segundo escenario viene referido al supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores. En tal caso, se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de la LOPD –se trata de lo que podemos denominar «cámaras identificadas no informadas»-.

El tercer escenario alude a la grabación de sonidos. Esta opción solo se admitirá si resultan "relevantes los riesgos para la seguridad de las instalaciones, bienes y personas" y si, además, se respeta "el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores".

Veamos con más detalle cada uno de ellos.

De entrada, si la empresa decide utilizar la videovigilancia como sistema de control del cumplimiento de las obligaciones laborales –obviamente, con el límite absoluto de las zonas prohibidas (89.2 LOPD)- y, por lo tanto, como sistema de obtención de prueba, debe, además de hacerlo en el ejercicio "legal y limitado de sus funciones", cumplir de manera previa con la obligación de información expresa y clara a los trabajadores y a sus representantes. Así pues, para entender válida desde la óptica procesal -art. 90.4 LRJS- la prueba obtenida mediante un sistema de videovigilancia será necesario:

1) Que el empresario ejerza su función de control legalmente y dentro de los límites relativos a la proporcionalidad, necesidad e idoneidad del sistema[41]. En este sentido, hay que tener en cuenta que la videovigilancia como sistema permanente y continuado de control no será admisible en general en las empresas[42].

2) Que el trabajador -y los representantes de los trabajadores si los hay- hayan sido informado de la finalidad de control de la actividad laboral a la que va dirigida la videovigilancia. Esta información deberá concretar las características y el alcance del tratamiento de datos que va a realizarse, esto es, en qué casos las grabaciones pueden ser

[41] Recordando la clásica STC 186/200, de 10 de julio, que se refería precisamente a videovigilancia, acreditada la justificación legítima del control -existían razonables sospechas de la comisión de graves irregularidades en el puesto de trabajo- cabe exigir, para entender válido en el marco del derecho a la intimidad personal, el recurso a esta medida que se acrediten sobre la misma tres requisitos: a) idoneidad para la finalidad pretendida por la empresa -verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes)-; b) necesidad -ya que la grabación serviría de prueba de tales irregularidades-; y, c) proporcionalidad –limitación espacial y temporal-.

[42] Así lo consideran MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* p. 139, que, en base a los Informes de la AEPD y a alguna resolución judicial, entiende que resultará desproporcionado un sistema de videovigilancia que permita el seguimiento continuo de la actividad laboral monitorizando por completo su actividad laboral; y, GARCÍA MURCIA, Joaquín y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde…", *op. cit.* p. 39, no parece que sea admisible, como regla general, una videovigilancia genérica y permanente con finalidad de control laboral, aunque se haga la oportuna advertencia a los trabajadores. La licitud de la medida de control no parece que pueda derivar de la mera voluntad del empleador, y la información previa a los trabajadores no parece que legitime por sí misma la actuación empresarial.

examinadas, durante cuánto tiempo y con qué propósitos, explicitando "muy particularmente" que pueden utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo[43].

Ahora bien, en segundo lugar, si no es la videovigilancia el sistema informado de control de las obligaciones laborales, en su párrafo segundo el art. 89.1 LOPD permite que la prueba obtenida a través de este medio pueda entenderse válida si constata "la comisión flagrante de un acto ilícito". En este caso, el único requisito que el precepto exige en relación con el deber de información es el recogido en el art. 22.4 LOPD que, como es sabido, se refiere a "la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679".

Con ello el legislador estaría admitiendo que, de manera excepcional y solo ante la comisión flagrante del ilícito, la prueba obtenida sería válida si el sistema de videovigilancia estaba identificado de modo ordinario, sin exigirse en este caso la información específica a que se refiere el primer párrafo del art. 89.1 LOPD[44].

A nuestro modo de ver, la regulación actual que configura estos dos niveles de videovigilancia asumiría de algún modo, por una parte, la doctrina constitucional – STC 29/2013, de 11 de febrero- que consideró insuficiente en el plano del derecho de protección de datos el hecho de que "existieran distintivos anunciando la instalación de cámaras y captación de imágenes" en el centro de trabajo, en el entendido de que "era

[43] En estos precisos términos STC 29/2013, de 11 de febrero. En este mismo sentido, considera SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 222, aunque la ley no exige que el empleador deba informar expresamente sobre la finalidad y el alcance concreto de la instalación, parece lógico pensar que se trata de uno de los contenidos esenciales que integran el deber de información empresarial, sin que la ley aclare, por otra parte, cuáles serían los efectos de un eventual incumplimiento del deber empresarial de información. Así, en sede de suplicación ya encontramos numerosas sentencias que, de acuerdo con lo previsto en el art. 89.1 LOPD, entienden lícita la prueba obtenida cuando "la empresa ha emitido con el Comité Intercentros acta conjunta para informar sobre las cámaras de videovigilancia y su utilización en actuaciones disciplinarias y que podrán ser utilizadas para la detección de acciones irregulares, sean éstas realizadas por personas ajenas a la empresa, por personal que presta servicios en la misma, sirviendo en su caso, como base para actuación disciplinaria laboral" (STSJ de Andalucía (Orden Social) de 11 de abril de 2019, rec. 1125/2018); o, por poner otro ejemplo, cuando se acredita que "la empresa llegó a un acuerdo con el Comité Intercentros sobre la existencia de cámaras de videovigilancia en los centros comerciales y de trabajo, en las zonas de trabajo, sean de acceso, tránsito, venta, elaboración o almacenamiento, muelle o aparcamiento, implantadas para controlar la seguridad de personas, bienes, instalaciones y mercancías a la venta, pudiendo ser utilizadas legítimamente para la detección de acciones irregulares, sean éstas realizadas por personas ajenas a la empresa, o por personal que presta servicios en la misma, sirviendo, en su caso como base para actuación disciplinaria laboral y dicho acuerdo se comunicó a los trabajadores a través de circulares internas colgadas en los tablones de anuncios y en el Sistema de Información de Empresa" (STSJ (Orden Social) de Madrid de 25 de enero de 2019, rec. 971/2018).

[44] Para GARCÍA MURCIA, Joaquín y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde…", *op. cit*. p. 39, este precepto es de redacción "un tanto equívoca y deficiente", pues en lugar de establecer una regla clara y precisa sobre el alcance de las facultades empresariales en esos casos, y sobre lo que puede hacer el empresario *ex ante* con esos fines de control particularizado, parte de la hipótesis de que en un momento determinado se haya captado, a través de los dispositivos existentes, la «comisión flagrante de un acto ilícito», en cuyo caso basta con la existencia de ese tipo de «dispositivos» para que se entienda cumplido el preceptivo deber de información.

necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida" y que, como es conocido, se refería a incumplimientos relacionados con la jornada de trabajo[45]; y, por otra parte, se ha de entender que esta nueva regulación asumiría y superaría a la vez la doctrina de la STC 39/2016, de 3 de marzo, pues no es posible sostener que si la instalación de la videovigilancia tiene por objeto controlar la actividad laboral, es válida la prueba obtenida de la misma "sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control" [46]. sin embargo, en breve aludiremos a ello, con la nueva regulación sí se admitiría que en el concreto supuesto que se cuestionaba en esta sentencia de 2016 –que, como también es sabido, se refería a la transgresión de la buena fe contractual por la comisión de pequeños hurtos- la prueba obtenida con cámaras identificadas y no informadas sería lícita en el plano del derecho del derecho de protección de datos.

En efecto, entendemos que cabe alcanzar esta doble conclusión porque, como ya hemos dicho, el cumplimiento de la obligación de información es condición esencial hoy desde la perspectiva de la licitud de la prueba si el sistema de videovigilancia se utiliza específicamente para el control de la actividad laboral. Por lo tanto, la mera identificación de la cámara en estos casos no sería hoy suficiente y, así, si la prueba obtenida se refiere al incumplimiento de las obligaciones laborales ordinarias y no a las vinculadas con la seguridad, cuando solo conste este único elemento informativo, deberemos considerar que, de acuerdo con el art. 89 LOPD, se ha vulnerado del derecho fundamental a la intimidad del trabajador.

De este modo, se ha de convenir en que la cuestión controvertida se centra tras la LOPD en la delimitación de lo que deba considerarse un ilícito flagrante porque, dado que nos movemos en un terreno relativo al respeto al derecho fundamental de protección de datos y de intimidad, será necesario acotar de modo preciso el espacio de la excepción a la regla general de la información previa, expresa, clara y concisa. Creemos pues que será necesario delimitar, en primer lugar, a qué ilícitos se refiere el art. 89.1.2ºparr (a); y, en segundo lugar, en qué casos debe considerarse flagrante su comisión (b).

[45] En contra de esta opinión SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p.223, que entiende que la excepción de las cámaras solo identificadas ampararía tanto el uso para fines disciplinarios de seguridad (personas, bienes o instalaciones) como la instalación temporal de cámaras con fines de control laboral cuando existieran fundadas sospechas previas de incumplimientos laborales. Interpretada en estos términos, la nueva regulación vendría a rectificar la doctrina del Tribunal Constitucional en el asunto Universidad de Sevilla (sentencia 29/2013, de 11 de febrero) y a otorgar carta de naturaleza, en cambio, a la doctrina del mismo Tribunal Constitucional en el caso Bershka (sentencia 39/2016, de 3 de marzo).

[46] Según esta STC "lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados". Un análisis extenso de la doctrina constitucional en materia de videovigilancia puede encontrarse en TALÉNS VISCONTI, Eduardo., "Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Volumen 6, núm. 3, julio-septiembre de 2018, p. 59 y ss.

a) Es evidente, por una parte, que no podemos identificar el ilícito a que se refiere el art. 89 LOPD con ilícito penal porque la tramitación parlamentaria de la LOPD nos lleva sin duda a esta conclusión[47]. En este sentido, como se ha apuntado[48], "aunque una lectura en clave tuitiva de la ley nos conduciría a interpretar restrictivamente la expresión "actos ilícitos", reservándola a los ilícitos de tipo penal, es lo cierto que tanto una interpretación literal como histórica de la ley, nos aboca a la interpretación contraria". Así pues, debemos entender que el ilícito sancionable a partir de la prueba videográfica identificada y no informada podrá tener o no relevancia a efectos penales. Y, en este punto, la cuestión a dilucidar pasa por concretar si deberá o no quedar acotado al ámbito de la protección por motivos seguridad o, dicho de otro modo, para la protección de las personas y las cosas; o si, dado que con ello también podríamos entender que nos movemos en el terreno penal, asumir que cualquier ilícito laboral captado por cámaras solo identificadas y no informadas debería considerarse obtenido lícitamente en los términos del art. 90.2 LRJS.

Consideramos que un argumento que el TS utilizó ya en 2017 podría servir también hoy para dar respuesta a esta cuestión en términos equilibrados desde la perspectiva del derecho fundamental a la intimidad. En la STS de 31 enero de 2017, rec. 3331/2015, se consideró que la prueba obtenida de cámaras de seguridad no específicamente utilizadas para el control laboral era "una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el logro de ese fin (control de cobros y de la caja en el caso concreto) y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc."[49].

De este modo, para el TS los incumplimientos laborales que deberían entenderse lícitamente probados mediante cámara identificada y no informada expresamente para controles laborales quedaban circunscritos a los relacionados con la seguridad de las cosas

[47] Como señala SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 225, el primer texto del proyecto de ley presentado por el Gobierno al Congreso se refería expresamente a la "comisión flagrante de un acto delictivo", de suerte que la nueva expresión empleada por la ley obedece claramente a la voluntad de extender la excepción prevista a cualquier supuesto de comisión flagrante de un incumplimiento laboral. En este sentido, TALÉNS VISCONTI, Eduardo., "Vídeo-vigilancia y protección de datos en el ámbito…", *op. cit.*, p. 84, comentando el texto del Proyecto de LOPD, consideraba que "esta excepción iría destinada para su valor probatorio en el proceso penal, en el sentido de que las imágenes captadas sin información probablemente no sirvan para sustentar una sanción laboral, pero sí que tendrían validez para una eventual sanción por la vía penal".

[48] SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 225

[49] Siguiendo esta doctrina jurisprudencial, los TSJ interpretan mayoritariamente que

o de las personas. En consecuencia, quedaban al margen de este ámbito de licitud las pruebas relacionadas con incumplimientos de las obligaciones laborales que podríamos denominar ordinarias y ajenas a la seguridad. En este sentido, el actual art. 89.2 LOPD debería interpretarse de manera restringida por lo que a los ilícitos laborales se refiere, haciendo una distinción entre:

- Obligaciones del trabajador referidas a condiciones de trabajo ordinarias: tiempo de trabajo, rendimiento, etc.
- Obligaciones de trabajo relativas al cumplimiento del deber de buena fe contractual respecto de la protección de las personas o las cosas.

El incumplimiento de las primeras detectado por cámaras no identificadas e informadas no podría ser sancionado lícitamente con la prueba obtenida de las mismas, debiendo entender que esta no podría considerarse válida por vulneración del derecho a la intimidad de los trabajadores en este caso. En cambio, el incumplimiento de las segundas detectado por cámaras identificadas y no informadas podría ser sancionado lícitamente con la prueba obtenida de las mismas, asumiendo que estos ilícitos laborales van más allá de la objetiva configuración de las obligaciones contractuales que ambas partes han de cumplir y que el empresario ha de controlar de modo ordinario. De hecho, el art. 22 LOPD, a cuyo apartado cuarto se remite el art. 89, regula precisamente a los sistemas de cámaras o videocámaras que se instalan con la finalidad de "preservar la seguridad de las personas y bienes, así como de sus instalaciones"[50].

b) Por lo que se refiere al carácter flagrante de la comisión del ilícito, cabría apuntar dos interpretaciones. Por una parte, de manera restrictiva, cabría entender que la conducta sancionable debería ser aquella que se descubre por la cámara identificada y no informada de manera sorpresiva e insospechada por la empresa. Evidentemente, en estos casos la obtención de la prueba debería considerarse lícita, puesto que conocida por el trabajador la existencia de la videocámara identificada, la comisión del ilícito que transgrede la buena fe contractual podrá ser sancionada porque se ajustará literalmente al "ilícito flagrante" a que se refiere el art. 89 LOPD.

No obstante, consideramos que cumplirá el requisito del carácter flagrante, el ilícito que se descubre por la videocámara identificada y no informada cuando esta se utiliza para controlar específicamente a partir de fundadas sospechas de alguna conducta irregular que se pueda estar cometiendo. En estos casos, la existencia de las cámaras sugiere, como señaló con claridad la STS de 7 de julio de 2016, rec. 3233/2014, "una finalidad protectora del patrimonio empresarial y la grabación de conductas que atenten contra esa finalidad";

[50] En este sentido, SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 223; para RODRÍGUEZ ESCANCIANO, Susana, "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales, *Diario La Ley*, Nº 9328, 2 de Enero de 2019 [versión digital], p. 5, "mayor será la posibilidad de supervisión cuanto más clara sea la fundada sospecha de comportamiento irregular por parte del empleado, pues no es igual comprobar el cumplimiento normal de las obligaciones laborales ordinarias, donde el deber de información debe de cumplimentarse en todos los extremos, que actuar ante el temor fundado de la perpetración de infracciones donde el principio de transparencia puede sufrir alguna modulación".

por lo que, ante sospechas que sirven como justificación legítima al empresario, la prueba obtenida de las mismas habrá de reputarse válida, ya que, continua la citada sentencia, "semejante entorno específico excluye el factor sorpresa y muestra claramente la situación de riesgo asumido por la demandante y por cualquier otro responsable de conductas análogas".

En definitiva, de acuerdo con los argumentos apuntados, la interpretación del segundo párrafo del art. 89.1 LOPD debe llevar a considerar, al menos así lo entendemos nosotros, que cabrá admitir, en los términos del art. 90.4 LRJS, las pruebas obtenidas con videocámaras identificadas y no informadas siempre y cuando se trate, por un lado, de ilícitos laborales que queden limitados a la transgresión de la buena fe contractual desde la perspectiva de la protección de las personas o las cosas en el ámbito de la empresa. Y, por otro, de ilícitos cometidos de manera flagrante y captados por las cámaras solo identificadas bien de manera sorpresiva –sin que se haya tenido previa sospecha de su concurrencia- bien tras un control más específico a partir de una justificación legítima de la empresa que actúa en base a determinados indicios de irregularidades.

Sentado lo anterior, aun quedaría una pregunta por responder en relación con el tema de la videovigilancia tras la LOPD: ¿Son admisibles las cámaras ocultas? ¿Puede la empresa recurrir a ellas ante sospechas de un ilícito laboral?

La respuesta inicial a estas cuestiones podría ser negativa en el entendido de que el art. 89 LOPD viene a limitar la opción legal de la videovigilancia «como mínimo» a las cámaras identificadas y no informadas y, en consecuencia, las cámaras ocultas no serían una opción en términos de licitud de la prueba obtenida porque implicarían en todo caso la vulneración del derecho fundamental a la intimidad.

Sin embargo, es obvio que la respuesta hoy debe formularse necesariamente a la luz de la doctrina del TEDH en la sentencia *López Ribalda II*. Como es sabido, con esta sentencia la Gran Sala modifica la interpretación que en la anterior resolución –STEDH (Sección Tercera) de 9 de enero de 2018[51]- consideró que, aunque la videovigilancia se había aplicado en el supuesto concreto ante sospechas legítimas de robo, su alcance fue amplio en el tiempo y desde una perspectiva subjetiva. Por lo tanto, se incumplía la regulación española de protección de datos de 1995 en relación con la obligación de información previa a los afectados respecto de la recogida y tratamiento de sus datos personales y de la existencia, finalidad y modalidades de la medida de vigilancia. De este modo, se declaró que los órganos jurisdiccionales españoles no habían ponderado adecuadamente los derechos de privacidad de las trabajadoras y otros intereses en juego, produciéndose, en consecuencia, una vulneración del artículo 8 CPDHLF.

Pues bien, siguiendo lo que se ha venido a llamar, con gran acierto, "un camino de ida y vuelta"[52], la STEDH (Gran Sala) de 17 octubre 2019, *Caso López Ribalda y otros contra*

[51] Un comentario de esta sentencia en TALÉNS VISCONTI, Eduardo., "Vídeo-vigilancia y protección de datos en el ámbito…", *op, cit.*, p. 61 y ss.

[52] MERCADER UGUINA, Jesús Rafael, "López Ribalda II: un camino de ida y vuelta", entrada de 30.10.19: https://forodelabos.blogspot.com/2019/10/lopez-ribalda-ii-un-camino-de-ida-y.html.

España, ha rectificado esta conclusión y ha venido a admitir la videovigilancia con cámara oculta, pero, como no podía ser de otro modo, de manera absolutamente condicionada. En este sentido, el pronunciamiento del TEDH se ha producido teniendo en cuenta los siguientes factores que nos parecen especialmente importantes:

- Que la doctrina *Barbulescu II* es aplicable *mutatis mutandis* a la videovigilancia (ap. 116)[53].

- Que, teniendo en cuenta esta doctrina, son claves para la admisión de la videovigilancia oculta, por una parte, el ámbito espacial, el temporal y el subjetivo (ap. 125 a 127); y, por otra, la prueba de que la información sobre las cámaras podía "poner en riesgo la finalidad de la videovigilancia" (ap. 128).

- A partir de la anterior afirmación, que la exigencia de transparencia y el derecho a la información son fundamentales en el contexto de las relaciones laborales, pero que la información proporcionada a la persona objeto de vigilancia y su alcance "son sólo uno de los criterios a considerar a la hora de valorar la proporcionalidad de tal medida en un caso determinado. Sin embargo, si falta esa información, las garantías derivadas de los demás criterios serán aún más importantes" (ap. 131).

- Y, en consecuencia, que no cabe aceptar que "la mínima sospecha de robos u otras irregularidades cometidas por los empleados, pueda justificar la instalación de un sistema de videovigilancia encubierta por parte del empleador", pero en las particulares circunstancias del caso planteado, las sospechas razonables de que se habían cometido "graves irregularidades" por la acción conjunta de varios empleados y "el alcance de los robos constatados" pueden parecer una justificación seria, teniendo en cuenta que esta situación podía crear en la empresa un clima general de desconfianza (ap. 134).

Con estas premisas, el Tribunal de Estrasburgo acaba considerando, en sentido contrario a la sentencia de 9 de enero de 2018, que en el caso planteado no se vulneró el art. 8 CPDHLF. Desde nuestro punto de vista, es posible extraer tres conclusiones tras esta resolución del TEDH que servirían, siempre desde la perspectiva del derecho fundamental a la protección de datos y a la intimidad, para confirmar de algún modo algunas de las afirmaciones que hemos hecho ya.

Estas tres conclusiones implican asumir que el espacio que el derecho a la intimidad deja al recurso de la videovigilancia como sistema de control es inversamente proporcional a la justificación legítima de la empresa. Dicho de otro modo, cuanto menor es esta mayor es el límite que perfila el derecho fundamental. Y así, si estamos ante un uso de la videovigilancia como medio de control del cumplimiento de las obligaciones laborales del trabajador, la justificación legítima sería también la elemental relacionada con el poder de dirección y control de la empresa. Sin embargo, si estamos ante un uso la videovigilancia como medio de control de un acto ilícito flagrante, la justificación

[53] En la sentencia se traslada el *test Barbulescu* al ámbito de la videovigilancia, incorporando las preguntas relacionadas con la proporcionalidad, necesidad e idoneidad a esta tecnología de control (véase, apartado 116).

legítima vendrá reforzada por la sospecha de la empresa y su derecho de protección de la seguridad de las personas y las cosas en la empresa.

De acuerdo con esto, tras la sentencia *López Ribalda II*, podríamos considerar, en primer lugar, que la videovigilancia como sistema de control ordinario en la empresa solo será posible en relación con el derecho a la intimidad del trabajador cuando se haya informado previamente de la existencia de las cámaras y de manera clara y exhaustiva sobre la finalidad del control y siempre dentro de los márgenes de la proporcionalidad, idoneidad y necesidad. En segundo lugar, que la videovigilancia identificada pero no informada será admisible cuando exista sospecha «siquiera mínima» de "robos o de otras irregularidades", esto es, cuando se vea afectada la protección de las personas o las cosas en clave de seguridad. Entendemos que cabe alcanzar esta segunda conclusión porque, en tercer lugar, para que quepa admitir que la videovigilancia oculta o encubierta no vulnera el derecho a la intimidad, el TEDH refuerza la sospecha que actúa como justificación legítima de la empresa al exigir que aquella sea de especial gravedad en el sentido de que "atente al buen funcionamiento de la empresa" y "al clima general de desconfianza en la empresa".

Para terminar con el análisis de este precepto legal, hemos de hacer mención especial a la grabación del sonido como dato especialmente protegido; porque el propio art. 89.3 LOPD así lo hace y además precisamente para aportar una estricta consideración de este control[54]. El precepto exige respecto de la grabación de sonidos, además de la aplicación de las garantías previstas en los apartados anteriores y que ya hemos analizado, tres condiciones:

- Que concurran relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo.

- Que la grabación respete el principio de proporcionalidad y el de intervención mínima.

- Que los sonidos conservados por estos sistemas de grabación se supriman en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Es evidente que, en relación con la grabación de la voz, el legislador ha tenido muy en cuenta la doctrina constitucional clásica porque se refuerza de manera especial en relación con el control que incluya el sonido tanto el requisito de la justificación legítima como el

[54] Como ha señalado RODRÍGUEZ ESCANCIANO, Susana., "Videovigilancia empresarial: límites a la…", *op. cit.*, p. 6, estos contornos más estrictos encuentran justificación en el solo hecho de tener en cuenta que las conversaciones están amparadas tanto por el derecho a la intimidad (art. 18.1 CE) cuanto por el derecho al secreto de las comunicaciones (art. 18.3 CE) y únicamente mediante autorización judicial es posible una injerencia en las mismas. La grabación de un diálogo suele ser más sensible que la de una imagen porque las palabras pueden revelar pensamientos y sentimientos internos, permitiendo comprobar fácilmente incumplimientos en el trabajo y adoptar medidas disciplinarias, de ahí que el Tribunal Europeo de Derechos Humanos –Asunto *Haldorf*- haya sido claro en la necesidad de que se avise al trabajador sobre la posible interceptación de los diálogos.

requisito de la proporcionalidad e intervención mínima[55]. En este sentido, la dicción literal del 89.3 LOPD acoge la argumentación de la conocida y clásica STC 98/2000, de 10 de abril, que, reconociendo la "utilidad" para la empresa de un sistema de control que graba el sonido, matiza 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". De este modo, la sentencia acaba considerando que la implantación de este sistema no resulta conforme "con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial" porque, sin ningún filtro, recoge todas las conversaciones que se producen en el lugar de trabajo. Así pues, de la sentencia se desprende claramente que la grabación del sonido afecta a un dato especialmente protegido porque "permite captar comentarios privados" lo que ha de considerarse "una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes"[56].

El art. 89.3 LOPD ha de ser interpretado a la luz de esta sentencia y, de ese modo, desde la perspectiva del art. 90.2 LRJS, habrá que entender que la licitud de la prueba en estos casos no será nada fácil de acreditar, dado que, primero, será necesario demostrar que la grabación del sonido responde a una justificación legítima reforzada y limitada a la seguridad. En segundo lugar, que el sistema que se utilice implica una intromisión lo menos invasiva posible. De este modo, queda descartado desde la perspectiva del derecho a la intimidad el uso de sistemas que permitan la audición continuada e indiscriminada de todo tipo de conversaciones. Y, en tercer lugar, deberá tratarse siempre de un sistema informado tanto a los trabajadores como a sus representantes, dado que el precepto declara aplicables las garantías previstas en los apartados anteriores[57].

4.3. El control del trabajador por geolocalización.

El control empresarial del cumplimiento de las obligaciones laborales mediante sistemas de geolocalización se contempla en el art. 90 LOPD; y habrá que estar a las exigencias contenidas en dicho precepto para valorar la licitud de la prueba. Pero vayamos por partes.

[55] SERRANO OLIVARES, Raquel., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.*, p. 224.

[56] En este sentido, recuerda MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* p. 147, que las grabaciones de sonido son especialmente sensibles porque con ellas se permite identificar a la persona, tal y como recoge la LOPD.

[57] MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.,* p. 148. Véanse en materia de información los Informes de la AEDP en esta materia que recoge el autor (p.148-149).

Para empezar, coincidimos con la mayor parte de la doctrina[58], en la crítica al legislador respecto de la regulación del control por geolocalización pues de la lectura del precepto no es posible articular un sistema fiable que asegure al trabajador un control en el marco de su derecho fundamental a la protección de datos y a la intimidad y a la empresa alguna garantía de que la obtención de la prueba será acorde a este derecho.

En efecto, en materia de control por geolocalización, el art. 90 LOPD ni de forma ordenada reconoce expresamente el derecho a la intimidad y a la protección de datos de los trabajadores, ni establece de manera precisa los límites al control empresarial. Según este precepto, la empresa podrá "tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo". Reitera así el legislador la referencia que vimos en el art. 87 respecto del uso de los dispositivos digitales y, dicho sea de paso, poco aporta por lo que a la geolocalización se refiere, porque con esta precisión de ejercicio legal del poder de control nada nuevo se nos dice.

En su apartado segundo el precepto hace alusión a la obligación de cumplir con el deber de información que asume la empresa indicando que esta deberá "de forma expresa, clara e inequívoca" informar a los trabajadores y, en su caso, a sus representantes, acerca de "la existencia y características de estos dispositivos". Igualmente deberá informarles acerca del "posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión". Se trata de una reiteración de las obligaciones que ya recoge en general en materia de protección de datos la LOPD de acuerdo con lo previsto en el Reglamento 2016/679. Por ello, cabe considerar que, en punto a la geolocalización, nos encontramos con un tratamiento débil desde la perspectiva del derecho fundamental de los trabajadores a la intimidad y a la protección de datos.

No obstante, desde nuestro punto de vista, es evidente que el art. 90 LOPD debe ser interpretado también, tal y como hemos considerado en relación con los dispositivos digitales y la videovigilancia, en línea con la doctrina de los Tribunales sobre la aplicación de los principios de justificación legítima, proporcionalidad, idoneidad y necesidad respecto de la instalación de sistemas de geolocalización como método de control de la

[58] MOLINA NAVARRETE, Cristóbal "Poder de geolocalización, intimidad y autodeterminación digital en las relaciones de trabajo: ¿un nuevo orden eficaz de garantías y límites?", *Diario La Ley*, núm. 9319, 2018, p.1 que considera que, al margen de las garantías comunes -obligación de información individual y la posibilidad de información colectiva subsidiaria), en la regulación de la geolocalización quedan ausentes las demás (obligación de causalidad específica para este dispositivo de control; principio de proporcionalidad; derecho a la participación de la representación los trabajadores en la fijación de los criterios de introducción y uso de los dispositivos digitales), lo que lleva a un problema de integración de estas lagunas "mediante la interpretación finalista y sistemática, por imperativos no sólo de coherencia legislativa sino constitucionales y comunitarios"; y, SERRANO OLIVARES, Raquel., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 225, que echa de menos tanto la referencia expresa a la finalidad y alcance de la instalación de tales dispositivos en cuanto contenido mínimo del deber/derecho de información, como la referencia expresa al principio de proporcionalidad como límite a la facultad empresarial de control.

actividad laboral. Además, puede resultar útil a efectos prácticos acudir, como hemos señalado también anteriormente, a los criterios que respecto del control por geolocalización ha recomendado el GT 29[59].

Por otra parte, dado que no tenemos doctrina jurisprudencial en materia de geolocalización y que se trata de un tema en el que el análisis casuístico es "imprescindible"[60], es importante acudir a la doctrina de suplicación, en tanto en cuanto, los Tribunales están interpretando en los últimos años de manera bastante equilibrada el alcance del poder empresarial de control mediante geolocalización aplicando precisamente los criterios que acabamos de reseñar.

Así, por ejemplo, en relación con la idoneidad de los sistemas de geolocalización se ha considerado que no cabe duda de que lo son cuando la actividad a controlar se desempeña a través del desplazamiento constante del trabajador -es paradigmático el caso de los comerciales-. De hecho, incluso se ha considerado desde el punto de vista de la proporcionalidad, una medida de control más ajustada a esta finalidad que otras posibles fórmulas que la empresa puede utilizar -control manual del cuentakilómetros, multas de tráfico que impongan los cuerpos policiales, las llamadas por teléfono de los clientes ante la inasistencia o retraso del trabajador, las llamadas por teléfono de los trabajadores una vez en el domicilio para dar de alta al cliente y comprobar el funcionamiento correcto del servicio de telecomunicaciones instalado o reparado, etc.[61]-, dado que es el sistema más eficiente para controlar tanto el destino de los vehículos como el modo de prestación del servicio para trabajadores que pasan buena parte de su jornada fuera de su centro de trabajo[62].

En todo caso, la doctrina judicial ha considerado de manera unánime que la información sobre el control empresarial del cumplimiento de las obligaciones laborales mediante geolocalización, resulta una condición esencial a la hora de valorar la licitud de la prueba obtenida por aplicación de este sistema en el marco del derecho fundamental de

[59] En este sentido, MERCADER UGUINA, Jesús Rafael, *Protección de datos y garantía de los derechos…, op. cit.*, p. 150.

[60] GARCÍA MURCIA, Jesús Rafael y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde…", *op. cit.* p. 40. Como señalan estos autores, la regulación no es suficientemente precisa, por cuanto en muchas ocasiones el dispositivo se implanta con la función de proteger bienes empresariales (v.gr., vehículo de empresa), pero a la vez permite conocer la ubicación y los movimientos del trabajador, algo que no parece haber previsto el legislador.

[61] En relación con la comparación de los sistemas de control, es muy interesante el análisis de la STSJ de Asturias (Orden Social) de 27 de diciembre de 2017 (rec. 2241/2017): "Los medios de control apuntados en el recurso suponen en gran medida dejar en manos de terceros -los cuerpos policiales que vigilan el tráfico, los clientes de la empresa- o de los propios trabajadores los mecanismos de supervisión y configuran un sistema de localización alternativo con lagunas e imperfecciones sobre el periodo de tiempo dedicado a los desplazamientos. La empresa debe tener la capacidad para sin acudir a ayudas externas, fundamentales en la propuesta del sindicato actor, organizar unos mecanismos efectivos de control y la utilización de dispositivos GPS en los vehículos de motor es un medio idóneo necesario y proporcionado a las características del desarrollo de la relación laboral. Además, aunque afecta a derechos fundamentales de los trabajadores su incidencia en ellos es de menos intensidad que otros posibles medios como el seguimiento por GPS instalado en el teléfono móvil utilizado en la prestación de servicios relación laboral".

[62] STSJ de la Comunidad Valenciana (Orden Social) de 2 de mayo de 2017 (rec. 3689/2016); o, STSJ de Asturias (Orden Social) de 27 de diciembre de 2017 (rec. 2241/2017).

protección de datos y de intimidad[63]. Así, la falta de información siempre se entiende contraria a estos derechos[64]. Es más, incluso cuando se acredita que la empresa sí ha transmitido de manera correcta y completa esta información, cabe considerar la vulneración del derecho fundamental si se constata que el control se extiende más allá de la jornada laboral[65].

En definitiva, con el nuevo art. 90 LOPD, no cabe duda de que en general puede mantenerse la interpretación que los Tribunales vienen haciendo respecto del uso de los sistemas de geolocalización en el marco del derecho fundamental a la protección de datos y a la intimidad.

5. Una breve reflexión final.

Es un hecho incuestionable que, en el marco de las facultades de organización y dirección inherentes a la empresa, ésta puede legítimamente regular el uso que hace el trabajador de los medios de titularidad empresarial que aquella pone a su disposición, prohibiendo, si así lo estima oportuno, su utilización para fines privados. Del mismo modo, la empresa ostenta la facultad de vigilar y controlar el cumplimiento de las obligaciones relativas a la utilización del medio de que se trate. Ahora bien, cualquier medida de supervisión debe implementarse con pleno respeto a la dignidad de los trabajadores y, por ende, a sus derechos fundamentales.

Teniendo en cuenta cual era la situación de partida, caracterizada por un ausencia de regulación casi absoluta, el establecimiento de previsiones normativas –art. 20 bis ET y, fundamentalmente, arts. 87 a 89 LOPD- en las que se regulan los procedimientos de control en el uso o frente al uso de dispositivos digitales en los que se puede ver afectado el derecho de protección de datos y el derecho a la intimidad de los trabajadores es, de por sí, un aspecto a valorar. Con el nuevo marco jurídico, los Tribunales de Justicia, a la hora de enjuiciar si el control empresarial ha sido ajustado a Derecho; o, más concretamente, si el procedimiento de obtención de la prueba ha sido o no respetuoso con el derecho fundamental de protección de datos y con el derecho de intimidad, deberán

[63] STSJ de Andalucía (Orden Social) de 28 de noviembre de 2018 (rec. 3827/2017).

[64] STSJ de Madrid (Orden Social) de 12 de julio de 2019 (rec. 197/2019) –en esta sentencia además el trabajador controlado por geolocalización no informada era delegado sindical, por lo que se entiende también vulnerado el derecho de libertad sindical-.

[65] De hecho, la STSJ de Asturias (Orden Social) de 27 de diciembre de 2017, que ya hemos ido analizando, concluye en la vulneración del derecho a la intimidad del trabajador porque este se mantenía activo cuando finalizaba la jornada laboral sin haber obtenido el consentimiento expreso del trabajador para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales conseguidos por ese medio: "La protección por la empresa de sus bienes y el control del uso que de ellos se haga una vez terminada la jornada de trabajo no constituye una excepción a la vigencia de la indicada regla general". En el mismo sentido, la STSJ de Andalucía (Orden social) de 19 de octubre de 2017 (rec. 1149/2017), declara vulnerado el derecho a la intimidad cuando el control se ha producido en relación a tramos horarios ajenos a la jornada laboral, como eran los periodos de baja por incapacidad temporal, para lo que no se encontraba autorizada la empresa.

comprobar si se han cumplido las exigencias que se contienen en los preceptos analizados de la LOPD.

Ahora bien, en el presente trabajo hemos podido comprobar que esta regulación no puede considerarse, ni mucho menos, adecuada desde la perspectiva del principio de seguridad jurídica que reconoce el art. 9.3 CE. Y la verdad es que, tratándose de una norma que regula perfiles de derechos fundamentales, esto resulta muy criticable. En este sentido, la crítica al legislador puede centrarse, en primer lugar, en la falta precisión a la hora de configurar la justificación legítima de la empresa para delimitar la intensidad del control. En segundo lugar, en la falta de recepción normativa eficiente de los principios clásicos de la doctrina constitucional de proporcionalidad, idoneidad y necesidad. Y, en tercer lugar, en la debilidad con la que se configura el derecho esencial de información que forma parte de aquellos derechos fundamentales.

Podríamos decir que da la impresión de que el legislador ha ido de más a menos en la redacción de los artículos 87, 89 y 90 LOPD. En el primero de los preceptos, de forma ordenada, reconoce primero el derecho a la intimidad del trabajador; en segundo lugar, el poder de control de la empresa; y, en tercer lugar, delimita el espacio de concurrencia de este derecho y este deber imponiendo límites a la empresa para que el control no supere el marco del derecho a la intimidad que el trabajador mantiene en el ámbito laboral. El segundo de los preceptos, de forma menos ordenada, no reconoce expresamente el derecho a la intimidad del trabajador, sino que comienza ya con el reconocimiento del poder de control empresarial. No obstante, limita este poder imponiendo la obligación de información, aunque no sin plantear importantes dudas interpretativas. Ahora bien, hay que destacar que, en relación con la grabación de sonidos, el legislador sí ha sido exhaustivo y sí ha cerrado la puerta a interpretaciones puesto que, tanto la justificación legítima como la proporcionalidad, la idoneidad y la necesidad de la medida de control están recogidas en el art. 89.3 LOPD. Todo lo contrario, ocurre con la regulación en relación con los sistemas de geolocalización, que garantiza débilmente el derecho del trabajador a la protección de datos y a la intimidad, planteando interrogantes en relación con la definición clara de los límites al control empresarial.

6. Bibliografía.

ARIAS DOMÍNGUEZ, Ángel y RUBIO SÁNCHEZ, Francisco, *El derecho de los trabajadores a la intimidad*, Aranzadi, Cizur Menor (Navarra), 2006.

BLASCO JOVER, Carolina., "Trabajadores "transparentes": la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados (I)", *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*, Volumen 6, núm. 3, julio-septiembre de 2018.

DE LOS COBOS ORIHUEL, Francisco. y GARCÍA RUBIO, Amparo. "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes

de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de los Derechos Humanos", en *Revista Española de Derecho del Trabajo*, núm. 196, 2017.

DESDENTADO BONETE, A. y DESDENTADO DAROCA, E., "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso *Barbulescu* y sus consecuencias sobre el control del uso laboral del ordenador", *Información Laboral*, 1/2018, BIB 2018\6059.

GARCÍA-PERROTE ESCARTÍN, Ignacio. "Ley, convenio colectivo, contrato de trabajo y derechos fundamentales del trabajador", *Revista de Derecho Social*, núm. 4, 1998.

GARCÍA-PERROTE ESCARTÍN, Ignacio.; Y MERCADER UGUINA, Jesús Rafael, "Conflicto y ponderación de los derechos fundamentales de contenido laboral", en AA.VV. (Dir. Sempere navarro, A.V, A.V), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003.

GARCÍA MURCIA, Joaquín. y RODRÍGUEZ CARDO, Iván Antonio, "La protección de los datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", Revista Española de Derecho del Trabajo, núm. 216, 2019.

GOERLICH PESET, Jose María., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico", en AA.VV. *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

GOERLICH PESET, José María "Poderes del Empresario", en AA.VV. (Coord. CAMPS RUÍZ, Luís. y RAMÍREZ MARTÍNEZ, Juan Manuel), *Derecho del Trabajo*, Tirant lo Blanch, Valencia, 2016.

GOÑI SEIN, Jose Luís., "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016, *Revista de Derecho Social*, núm. 78, 2017.

MERCADER UGUINA, Jesús Rafael., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Ed. Francis Lefebvre. Claves Prácticas, Madrid, 2019.

MERCADER UGUINA, Jesús Rafael, "López Ribalda II: un camino de ida y vuelta", entrada de 30.10.19: https://forodelabos.blogspot.com/2019/10/lopez-ribalda-ii-un-camino-de-ida-y.html.

MOLINA NAVARRETE, Cristóbal "Poder de geolocalización, intimidad y autodeterminación digital en las relaciones de trabajo: ¿un nuevo orden eficaz de garantías y límites?", *Diario La Ley*, núm. 9319, 2018.

PALOMEQUE LÓPEZ, Manuel Carlos, "Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos", en AA.VV. (Dir. SEMPERE NAVARRO, Antonio Vicente), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003.

PRADOS DE REYES, Francisco Javier, "Contrato y relación de trabajo", en AA.VV., *Veinte años de jurisprudencia laboral y social del Tribunal Constitucional*, Tecnos, Madrid, 2001.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, Miguel. "La integración de los derechos fundamentales en el contrato de trabajo", en AA.VV. (Dir. SEMPERE NAVARRO, Antonio Vicente), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003.

RODRÍGUEZ ESCANCIANO, Susana, "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales, *Diario La Ley*, Nº 9328, 2 de Enero de 2019.

SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *IusLabor,* 3/2018.

TALÉNS VISCONTI, Eduardo., "Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo,* Volumen 6, núm. 3, julio-septiembre de 2018.

TERRADILLOS ORMAETXEA, Edurne., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social*, n. 80, 2017.

URRUTIA SAGARDÍA, Eneko. "Importancia estratégica del *Big Data*", *Actualidad Jurídica Aranzadi*, núm. 935, 2017

VALDÉS DAL-RÉ, Fernando, "Poderes del empresario y derechos de la persona del trabajador", *Relaciones Laborales*, 1990, núm. 1.