Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa

Business technological control and new application problems after the L.O. 3/2018. A look from the duty of previous information

María Amparo García Rubio*
Profesora Titular de Derecho del Trabajo y de la Seguridad Social
Universitat de València

Recibido: 15/2/2022
Aceptado: 10/3/2022
doi: https://doi.org/10.20318/labos.2022.6845

Resumen: La aprobación de la L.O. 3/2018, de Protección de datos personales y garantía de los derechos digitales, ha puesto fin a la situación previa de ausencia de regulación legal específica en materia de control tecnológico en la relación laboral. No obstante, la llegada de esta Ley no ha acabado con todos los interrogantes que la cuestión plantea, no sólo por las dudas interpretativas que generan algunas de sus previsiones, sino también porque ahora es necesario determinar la relación entre ese nuevo parámetro de legalidad y el canon de constitucionalidad. Estas controversias se están haciendo visibles en la práctica judicial, de ahí que el presente estudio se dirija a profundizar en esos nuevos conflictos suscitados, con especial atención a los vinculados al deber empresarial de información.

Palabras clave: dispositivos digitales, geolocalización, videovigilancia, derechos fundamentales, relación laboral

Abstract: The approval of the L.O. 3/2018, Protection of personal data and guarantee of digital rights, has ended the previous situation of absence of specific legal regulation on technological control in the labour relation. However, the arrival of this Law has not eliminated all the questions that the matter raises, not only because of the interpretative doubts generated by some of its provisions, but also because it is now necessary to determine the relationship between this new parameter of legality

*amparo.garcia-rubio@uv.es

and the constitutional canon. These controversies are becoming visible in judicial practice, hence the present study is aimed at delving into these new conflicts, with special attention to those linked to the corporate duty of information.

Keywords: digital devices, geolocation, video surveillance, fundamental rights, labour relation.

1. Control tecnológico y derechos fundamentales: el conflicto como punto de partida

El objeto del presente estudio es el de realizar una reflexión general sobre los parámetros actuales –normativos y jurisprudenciales– a los que debe sujetarse el control que las empresas pueden realizar sobre la actividad laboral mediante medios tecnológicos, en virtud de sus facultades de dirección y vigilancia vinculadas a derechos constitucionales como la propiedad y la libertad de empresa (arts. 33 y 38 CE)[1]. Más en concreto, y como suele ser habitual, el propósito final es el de ahondar en los límites a los que ese control debe someterse en el marco vigente, en aras a salvaguardar los derechos fundamentales de las personas trabajadoras con los que dichas facultades empresariales entran en conflicto: básicamente, su derecho a la intimidad; en su caso, el derecho al secreto de las comunicaciones; y prácticamente en todos los casos, el derecho a la protección de datos personales, que, por la amplitud dada a su objeto, se ha convertido en el gran protagonista a considerar (art 18 CE).

Estamos ante una cuestión que en los últimos años se ha visto afectada por sucesivas novedades, tanto jurisprudenciales como normativas. En este último terreno, el hito más relevante ha sido la aprobación de los arts. 87 a 91 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales (LOPD) –norma legal mediante la que se pretende la adaptación al Reglamento (UE) 2016/679, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE–. Estos preceptos legales han reconocido la facultad empresarial de realizar el control de la actividad laboral a través de dispositivos digitales, geolocalización y videovigilancia. Directamente, por tanto, el legislador ha admitido posibles limitaciones a los derechos fundamentales de las personas trabajadoras. Sin embargo, lo que ya no ha acabado de concretar con precisión son los parámetros a aplicar para determinar si esas restricciones son conformes a Derecho.

Precisamente, sobre este último aspecto se centrará el análisis que sigue. En él, con carácter transversal para los diversos medios tecnológicos de vigilancia, tratará de determinarse cuál es en la actualidad el canon de enjuiciamiento común a aplicar a ese control empresarial a efectos de decidir si es o no legítimo, esto es, si es o no respetuoso con los derechos fundamentales de las personas trabajadoras, y en consecuencia, si la

[1] SSTC 92/1992, de 11 de junio, FJ 3; 57/1999, de 12 de abril, FJ 8; 107/2000, de 5 de mayo, FJ 7; 241/2012, de 17 de diciembre, FJ 4; 39/2016, de 3 de marzo, FJ 4.

prueba que de él derive podrá o no ser válida para acreditar eventuales incumplimientos laborales que pudieran detectarse (arts. 11.1 LOPJ y 90.2 LJS). Para ello, a partir de los problemas previos, la pretensión principal es reflexionar sobre las nuevas controversias interpretativas que la llegada de la LOPD y su aplicación judicial están suscitando en el conflicto de derechos señalado, con particular atención a la incidencia que sobre la validez de esa vigilancia ejercen las deficiencias en la previa información de dicho control.

2. El canon de enjuiciamiento sobre el control tecnológico empresarial

A día de hoy, dado el valor interpretativo que los pronunciamientos de los Tribunales supranacionales tienen sobre nuestros derechos fundamentales (art. 10.2 CE), el canon de enjuiciamiento sobre la "tecnovigilancia" empresarial viene determinado, no sólo por lo establecido a nivel interno y, en particular, por nuestro Tribunal Constitucional, sino también, entre otros, por las resoluciones del Tribunal Europeo de Derechos Humanos, cuya doctrina al respecto se ha establecido en los últimos años, fundamentalmente, a través de dos conocidos pronunciamientos: por un lado, la STEDH Bărbulescu II, de 5 de septiembre de 2017, dictada en materia de monitorización de ordenadores, y por otro, como complemento de la anterior, la STEDH López Ribalda II, de 17 de octubre de 2019, emitida en un supuesto de videovigilancia. A partir de este bloque jurisprudencial es posible dejar sentadas dos ideas iniciales que resultan básicas en el análisis.

2.1. Irrelevancia de la finalidad inicial del medio de control

La primera idea es que, tras la STEDH Bărbulescu II, queda confirmado que el canon de enjuiciamiento a aplicar es el mismo con independencia de la finalidad originaria del instrumento de control.

Obviamente, ese canon se aplica cuando la fiscalización se realiza a través de instrumentos instalados directamente para vigilar: es el caso de las videocámaras, y por lo general, aunque pueda tener otras prestaciones, también de los geolocalizadores.

Pero, además, ese mismo canon de enjuiciamiento se va a aplicar al control que recae sobre instrumentos que en principio se proporcionan por los empresarios como meras herramientas de trabajo: es el caso de los dispositivos digitales –ordenadores y análogos–. También la vigilancia empresarial sobre ellos queda sujeta a límites. De este modo, restricciones que el empresario no tiene para inspeccionar otro tipo de maquinaria o para inspeccionar documentación elaborada por los trabajadores en formato papel, sin embargo, cuando esa misma documentación está en un ordenador, entonces el empresario ve recortada su facultad de control. Necesariamente cabe preguntarse por la razón de esta diferencia. Pues bien, seguramente, esto es así porque se presume que los trabajadores pueden utilizar estas herramientas de trabajo con fines privados, de modo que en el espacio del ordenador no sólo se halle información laboral, sino también perso-

nal. En ocasiones, ese uso privado será lícito porque así se haya tolerado o admitido por la empresa. Pero incluso aunque haya mediado una prohibición expresa de uso privado y este sea por tanto ilícito, también ahí el control empresarial queda sujeto a restricciones.

Esta es una conclusión derivada de la STEDH Bărbulescu II, que en su momento resultó fundamental a nivel interno, dado que venía a corregir o matizar de forma considerable lo hasta entonces dicho por nuestro Tribunal Constitucional en sus SSTC 241/2012, de 17 de diciembre, y 170/2013, de 7 de octubre. En estos pronunciamientos se había mantenido que si en la empresa regía una prohibición expresa de uso privado de los dispositivos digitales, los trabajadores carecían de una expectativa de privacidad y de confidencialidad sobre la información allí contenida, pues esa prohibición llevaba implícita la facultad del empresario de controlar la utilización de tales herramientas, de ahí que se considerara un ámbito que quedaba fuera de la protección del derecho a la intimidad y, también, del derecho al secreto de las comunicaciones, pues se entendía que ese canal de comunicación no era cerrado, sino abierto a la posible fiscalización empresarial. Esta idea, sin embargo, pese a que se sigue deslizando en algunas sentencias de nuestros tribunales ordinarios[2], parece difícil de mantener tras la STEDH Bărbulescu II. En esta Sentencia, el Tribunal Europeo señaló que las instrucciones de la empresa no anulan estos derechos de las personas trabajadoras y que, aunque hubiera habido prohibición de uso personal de los ordenadores de la empresa, el control empresarial se hallaba limitado y sólo sería legítimo si superaba una serie de garantías y exigencias.

En consecuencia, y como se ha apuntado al inicio, esta aportación jurisprudencial implica que, a día de hoy, el canon de enjuiciamiento resulte común, con independencia de la finalidad inicial del instrumento mediante el que se materialice el control tecnológico empresarial –esto es, sea o no una herramienta de trabajo–.

2.2. Parámetros integrantes

Con relación a esas garantías y exigencias que actúan como límite, la segunda idea que se confirma tras la STEDH Bărbulescu II es que el canon de enjuiciamiento a aplicar al control tecnológico empresarial para medir si es o no legítimo queda configurado o compuesto por dos elementos.

a) El primero es el clásico principio de proporcionalidad, que desde siempre ha sido el criterio utilizado por nuestro Tribunal Constitucional, y que se integra por diversos ítems que, con independencia de cómo los sistematice y denomine el TEDH, en esencia vienen a coincidir con los mismos juicios tradicionalmente exigidos por la jurisprudencia constitucional interna para estimar que una medida de control empresarial, limitativa de derechos fundamentales de los trabajadores, resulta legítima: esto es, que esa medida empresarial esté justificada por un interés legítimo; que sea idónea para

[2] SSTS de 8 de febrero de 2018 (Rº. 1121/2015, Sala de lo Social); de 15 de septiembre de 2020 (Rº. 528/2018, Sala de lo Social); STSJ de C. Valenciana, de 3 de febrero de 2021 (Rº. 2159/2020).

conseguir el objetivo propuesto; que supere el juicio de necesidad, en el sentido de que no exista otra medida más moderada para conseguir el propósito buscado con igual eficacia; y, finalmente, que la medida sea ponderada o equilibrada, es decir, que el grado de intrusión o restricción del derecho fundamental no haya ido objetiva y temporalmente más allá de lo estrictamente necesario en atención a la razón que motivó el control –básicamente, que no se acceda a más contenidos o datos de los imprescindibles, o no se extienda el control durante más tiempo del indispensable–[3].

Curiosamente, a salvo de una mínima mención realizada respecto a la grabación de sonidos, los arts. 87, 89 y 90 LOPD no hacen ninguna referencia al principio de proporcionalidad[4]. No obstante, pese a ese silencio legal, no hay duda de su aplicación, y de hecho, como después se constatará, sigue constituyendo el principal canon para medir la legitimidad del control empresarial.

b) Pero junto al anterior y sobradamente conocido principio, desde la STEDH Bărbulescu II también se deja claro que, de forma adicional, el enjuiciamiento de la legitimidad de la vigilancia empresarial debe además atender a un segundo elemento para apreciar su validez: se trata de constatar que, con carácter previo a su aplicación, la empresa ha informado a las personas trabajadoras sobre la existencia de medidas de control tecnológico –en su caso, posible monitorización de ordenadores, y/o instalación de cámaras y geolocalizadores–, así como su alcance.

En su momento, esta aportación de la jurisprudencia europea también resultó muy relevante puesto que, hasta entonces, nuestro Tribunal Supremo y nuestro Tribunal Constitucional habían seguido una línea zigzagueante respecto a la exigencia de este requisito en la validez de la vigilancia laboral[5]. Desde la STEDH Bărbulescu II queda ya

[3] Por todas, SSTC 186/2000, de 10 de julio; 39/2016, de 3 de marzo.

[4] En cambio, respecto al trabajo a distancia, la Ley 10/2021 sí hace mención a "los principios de idoneidad, necesidad y proporcionalidad" como límite al control de la prestación laboral mediante dispositivos automáticos y telemáticos (art. 17.1).

[5] Así, respecto a la inspección de ordenadores, y con relación a los derechos a la intimidad y al secreto de las comunicaciones, el *iter* jurisprudencial había sido el siguiente. De inicio, la STS de 26 de septiembre de 2007 (Rº. 966/2006, Sala de lo Social) –reiterada por la STS de 8 de marzo de 2011 (Rº. 1826/2010)–, supeditó la validez de la vigilancia a que la empresa hubiera informado previamente, no sólo de las reglas de uso de los medios informáticos, sino también de los posibles controles empresariales a realizar para comprobar su correcta utilización. En cambio, la STS de 6 de octubre de 2011 (Rº. 4053/2010, Sala de lo Social), señaló que la legitimidad de la medida empresarial sólo requería que la empresa hubiera informado previamente sobre la prohibición de uso personal de los medios informáticos puestos a disposición de los trabajadores, sin necesidad de que hubiera también advertido de los eventuales controles a realizar. Este último criterio es el que después se reflejó en las ya citadas SSTC 241/2012 y 170/2013.

Con relación a medidas de audio y videovigilancia laboral, las SSTC 98/2000, de 10 de abril, y 186/2000, de 10 de julio, adoptaron como canon de control de constitucionalidad el del principio de proporcionalidad para enjuiciar su adecuación al derecho a la intimidad, declarándose en la segunda de estas sentencias la irrelevancia constitucional de no haber comunicado su instalación a los trabajadores y sus representantes. Ya con relación al derecho a la protección de datos, se partía de que el contenido de este derecho exige informar a los interesados, pero mientras la STC 29/2013, de 11 de febrero, no consideró suficiente el cartel anunciador de las cámaras y exigió como requisito de validez haber comunicado previamente a los trabajadores sus posibles efectos disciplinarios, sin hacer ninguna otra ponderación, la STC 39/2016, de 3

claro que, en el canon de enjuiciamiento del control empresarial, no sólo se incluye la superación del principio de proporcionalidad, sino que también ha de atenderse a si la empresa ha cumplido con esa exigencia de información previa.

Este segundo componente del canon de enjuiciamiento, relativamente más novedoso, es objeto de atención más detenida en los siguientes epígrafes. Tal interés se justifica por dos razones. La primera porque examinar el tratamiento dado por la LOPD a este requisito en cada uno de los tres medios de control tecnológico regulados en esta Ley –dispositivos digitales, geolocalización y videovigilancia– puede servir de hilo conductor para realizar un repaso general al régimen jurídico previsto por el legislador para cada uno de estos instrumentos de vigilancia. El segundo motivo para profundizar en esta exigencia responde a que, probablemente, es uno de los aspectos que más problemas está provocando o va a provocar en la práctica judicial en la materia: por una parte, por las insuficiencias o deficiencias técnicas de su regulación legal, y por otra parte, porque, paradójicamente, después de estar años reivindicando una normativa específica que regulara el control tecnológico en el ámbito de las relaciones laborales, ahora que ya la tenemos surge el problema de determinar la articulación entre ese plano legal y el plano constitucional.

En consecuencia, en las líneas que siguen se procederá al examen de los siguientes puntos. En primer lugar, se aludirá a la regulación legal del requisito de información previa en cada uno de los tres medios de control tecnológico regulados en la LOPD, haciendo especial referencia a los interrogantes que su interpretación plantea. Seguidamente, se analizarán las consecuencias de su incumplimiento para, en concreto, determinar si toda infracción legal respecto a esa exigencia constituye o no una vulneración constitucional de los derechos fundamentales de las personas trabajadoras, y por tanto, si toda inobservancia total o parcial de ese régimen legal del requisito de información previa va a conllevar o no la nulidad de la prueba derivada.

3. El requisito de información previa en la LOPD

En nuestra legislación interna, la LOPD aborda el deber de información sobre el tratamiento de datos personales a un doble nivel: por un lado, contiene una regulación general para cualquier ámbito; y por otro lado, y en lo que aquí interesa, incluye previsiones específicas cuando regula las garantías de los derechos digitales en el ámbito laboral.

a) Respecto a la primera, la normativa general sobre protección de datos personales regula ese deber de información en los términos establecidos en los arts. 11 y 22.4 LOPD y en los arts. 12 a 14 Reglamento [UE] 2016/679. Tales preceptos imponen que, cuando los datos personales sean obtenidos de los interesados, dicha información ha de

de marzo, por el contrario, sí consideró bastante el distintivo informativo, y aunque no hubiera mediado información previa de sus fines sancionadores, admitió que la videovigilancia laboral no vulneraba dicho derecho *ex* art. 18.4 CE, y además consideró respetado el derecho a la intimidad tras constatar la superación del juicio de proporcionalidad.

facilitarse "en el momento en que estos se obtengan", admitiéndose que, cuando no son obtenidos del interesado, la información podrá proporcionarse con posterioridad en los márgenes del art. 14.3 del Reglamento comunitario. Asimismo, esa normativa exige incluir en la información una serie de indicaciones, entre las que se encuentra la de expresar la finalidad del tratamiento.

A efectos de consideraciones posteriores, respecto a esta última indicación es importante señalar que, de acuerdo también con esa normativa general, los fines de la recogida de datos deben ser "determinados, explícitos y legítimos", y como regla general queda vedado que, con posterioridad, esos datos sean tratados "de manera incompatible con dichos fines" (art. 5.1.b Reglamento [UE] 2016/679[6]). Cierto es que, conforme al vigente tenor, no se prohíbe todo tratamiento para finalidad distinta, sino para finalidad incompatible. Se trata, no obstante, de una frontera de difícil delimitación, que no siempre encuentra claro reflejo en nuestra práctica judicial interna[7]. No hay que olvidar que, en diversos pronunciamientos, el Tribunal Constitucional ha afirmado que el derecho a la protección de datos personales comprende "la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[8]. En todo caso, el propio Reglamento [UE] 2016/679 ofrece algunos criterios a considerar para determinar la posible compatibilidad entre finalidades diferentes (art. 6.4), y entre ellos, en el ámbito laboral cobra especial importancia el referido a "las posibles consecuencias para los interesados del tratamiento ulterior previsto". En tal sentido, desde la perspectiva de las personas trabajadoras, piénsese en la relevancia de los efectos sancionadores derivados de un uso con fines de control laboral *ex* art. 20.3 ET cuando en un principio se informó para finalidad diferente, siendo evidentes las consecuencias perjudiciales que para los interesados se desencadenan a partir de esa nueva finalidad –ello, al margen de que cuanto más se aleja el tratamiento de la finalidad inicial más se desvirtúa la exigencia de informar del fin determinado y explícito del tratamiento, si bien, los arts. 13.3 y 14.4 Reglamento [UE] 2016/679 ordenan que si se procede al tratamiento ulterior de datos personales "para un fin que no sea aquel para el que se recogieron", habrá de proporcionarse información al interesado sobre ese otro fin "con anterioridad a dicho tratamiento ulterior"–.

b) En todo caso, respecto a ese ámbito de las relaciones laborales, la regulación específica contenida en los arts. 87, 89 y 90 LOPD incorpora previsiones particulares relativas al deber empresarial de información.

Con relación a ese régimen legal propio, lo primero que llama la atención en la LOPD es el distinto alcance que, como seguidamente se verá, el legislador ha dado al requisito de información previa en cada uno de los tres medios de control tecnológico regulados, sin que se acabe de esclarecer el carácter complementario o no que tienen las reglas generales respecto a cada una de esas regulaciones específicas.

[6] Cfr. art. 72.1.d) LOPD.

[7] *Vid.* SAN de 22 de febrero de 2019 (Rº. 372/2017, Sala de lo Contencioso-administrativo).

[8] STC 292/2000, de 30 de noviembre, FJ 5; o SSTC 58/2018, de 4 de junio, FJ 5; 76/2019, de 22 de mayo, FJ 6.

3.1. Alcance en el control sobre dispositivos digitales

Cuando se trata de la inspección de ordenadores o dispositivos similares facilitados por la empresa, el art. 87 LOPD sólo alude a la obligación empresarial de "establecer criterios de utilización de los dispositivos digitales", en los términos expresados en su apartado 3. De esta expresión se deduce que el legislador impone al empresario informar sobre la política de uso de los dispositivos digitales que rige en la empresa, es decir, si su uso está absolutamente prohibido para fines personales de los trabajadores –opción que, frente a opiniones contrarias[9], a mi juicio resulta jurídicamente posible[10]– o si, por el contrario, el empresario apuesta por la alternativa opuesta de permitir su utilización para fines privados. En este último caso, lo único que añade el precepto es que se precisen esos usos autorizados y se establezcan garantías en favor de la intimidad de los trabajadores, como, en particular, que se determinen los períodos en que ese uso personal se tolera.

A mi juicio, y aunque tampoco constituya cuestión pacífica[11], el tenor del precepto legal no explicita la exigencia de que la empresa proporcione información previa a las personas trabajadoras sobre el control a través de dispositivos digitales y su alcance[12]. Cabría, no obstante, plantearse si tal obligación pudiera derivar de la normativa general sobre protección de datos personales. Ahora bien, para alcanzar una respuesta afirmativa a tal cuestión, previamente habrían de superarse ciertos obstáculos.

De entrada, habría de admitirse que el tenor del art. 87 LOPD –con referencia exclusiva al derecho a la intimidad– y la letra del art. 2.1 LOPD –con mención únicamente a la aplicación de sus Títulos I a IX y sus arts. "89 a 94" al tratamiento de datos personales– no imposibilitan la proyección de la normativa general de esta Ley al uso de los dispositivos digitales. A mi juicio, la literalidad de estas previsiones no impediría tal proyección desde el momento en que el acceso a esas herramientas informáticas implique el tratamiento de datos personales, premisa esta que ha venido siendo tradicionalmente admitida por el, en su momento, denominado Grupo de Trabajo del art. 29 de la Directiva 95/46/CE[13]. En tal sentido actuaría también el posterior art. 17.1 Ley 10/2021, que,

---

[9] *Vid.* ORELLANA CANO, A.M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores*, Aranzadi, Navarra, 2019, p. 170; RODRÍGUEZ ESCANCIANO, S., "Participación de los representantes de los trabajadores en el tratamiento de datos personales: derechos de información y consulta", *Jurisdicción social. Revista de la Comisión de lo Social de Juezas y Jueces para la Democracia*, nº 197, 2019, p. 48.

[10] Respecto al razonamiento de esta afirmación, me remito a lo expuesto con más detalle en GARCÍA RUBIO, M.A., "El control sobre el uso de los ordenadores puestos a disposición de los trabajadores", en TALÉNS VISCONTI, E.E. y VALLS GENOVARD, M.A. (Dir.), *La actividad de los detectives privados en el ámbito laboral. Aspectos sustantivos y procesales de la obtención de la prueba*, Bosch Wolters Kluwer, Madrid, 2020, pp. 150-151.

[11] *Vid.* BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho* nº 54/2019, smarteca, p. 12.

[12] *Vid.* SERRANO OLIVARES, R., "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, p. 220.

[13] En su Dictamen 8/2001 (WP48), sobre el tratamiento de datos personales en el contexto laboral, afirmó que la monitorización por el empresario del correo electrónico de los trabajadores o del acceso a internet

dentro del capítulo dedicado a los "derechos de las personas trabajadoras a distancia", señala que "la utilización de los medios telemáticos y el control de la prestación laboral mediante dispositivos automáticos garantizará adecuadamente el derecho a la intimidad *y a la protección de datos, en los términos previstos en la Ley Orgánica 3/2018*". Sucede, sin embargo, que tras la LOPD se ha afirmado por parte de la Agencia Española de Protección de Datos (AEPD) que, a la vista de los comentados preceptos de esta Ley y con relación a su Título X, "el propio legislador está reconociendo que solo en los casos de los artículos 89 a 94 nos encontraríamos ante tratamientos de datos de carácter personal y, por ende, en el ámbito competencial de la AEPD", habiendo explicitado que entre los derechos que considera "completamente ajenos a las competencias de la AEPD al no guardar relación con la protección de datos personales" se incluye el "derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (Artículo 87)"[14].

Con todo, aun cuando, en virtud de lo dicho, se admita la aplicación de la normativa general sobre protección de datos al acceso a los dispositivos digitales, la exigencia de información sobre el control "en el momento en que estos se obtengan" –y no en márgenes posteriores– requeriría admitir la interpretación de que tales datos personales se obtienen de los interesados, lectura esta que parece podría encontrar cobertura en lo que el citado Grupo de Trabajo del art. 29 denomina datos obtenidos del interesado "mediante observación" (art. 13 Reglamento [UE] 2016/679)[15]. Desde la hipótesis de partida, tal premisa, como se indica, obligaría a informar del tratamiento de datos personales "en el momento en que estos se obtengan", expresión distinta a la contenida en el antiguo art. 5.1 L.O.

queda dentro de la tutela del derecho a la protección de datos. Tal dictamen se completó por dicho Grupo del art. 29 con el Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo (WP55) de 2002, y mediante el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo.

Por su parte, la Agencia Española de Protección de Datos también ha confirmado este criterio: *v.gr.* Resolución R/02615/2010 –información sobre accesos a internet–; Informe 0437/2010 –dirección de correo electrónico corporativo–; Resolución E/04495/2012 –datos derivados de controles sobre ordenador y correo electrónico–.

En la doctrina científica, GOÑI SEIN, J.L., "Uso de los dispositivos digitales en el ámbito laboral", *Trabajo y Derecho* nº 11/2020, smarteca, pp. 20-22, integra el art. 87.3 LOPD con el Reglamento [UE] 2016/679 y, en particular, con las exigencias de información previstas en sus arts. 13 y 14. También NAVARRO NIETO, F., "Facultades empresariales y garantías del trabajador en relación con el uso de dispositivos digitales en el ámbito laboral", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021, p. 252, afirma que la escueta referencia del párrafo 3º del art. 87.3 LOPD al derecho a la información de los trabajadores "debe ser interpretada en su alcance conforme al deber de transparencia delimitado normativamente (art. 5 RGPD)", aplicando analógicamente las exigencias informativas previstas para otros medios de control en los arts. 89.1 y 90.2 LOPD.

[14] Resolución de 22 de enero de 2021 en el procedimiento E/00377/2020. Asimismo, *vid.* Resoluciones de 12 y 21 de agosto de 2020 en el procedimiento E/10250/2019.

[15] De acuerdo con las "Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679" (WP260 rev.01, revisión de 11 de abril de 2018), el art. 13 del Reglamento [UE] 2016/679 se aplica a la situación en la que los datos se obtienen del interesado, lo que entiende incluye los datos personales que "un responsable del tratamiento obtiene de un interesado mediante observación (p. ej., utilizando dispositivos automáticos de captura de datos o programas informáticos de captura de datos, como por ejemplo cámaras, equipos de red, localización por wifi, RFID u otros tipos de sensores)".

15/1999 y que para entender que impone la información "previa" requeriría interpretar que, más allá de la simultaneidad, exige su comunicación antes de iniciarse la recogida de datos, conforme en algún momento ha admitido la AEPD[16]. En todo caso, y llegados a este punto, la aceptación de la aplicación de la normativa general de protección de datos sí impondría que tal información debiera contener todas las indicaciones requeridas por aquélla, incluida la de comunicar la finalidad del tratamiento –conforme al art. 87.2 LOPD, sólo la de controlar el cumplimiento de las obligaciones laborales o la de garantizar la integridad de dichos dispositivos–, rigiendo por tanto el comentado principio de limitación de la finalidad.

Sin duda, tantos obstáculos a superar y tantas premisas a aceptar no se avienen bien con la seguridad jurídica. En cualquier caso, pese a esa ambigüedad del régimen legal respecto al deber de la empresa de informar previamente a los trabajadores sobre la fiscalización mediante dispositivos digitales, lo cierto es que, si nos situamos en el plano constitucional de legitimidad de ese control, necesariamente ha de aconsejarse a las empresas que proporcionen dicha información previa, pues, a la vista de lo dicho en la STEDH Bărbulescu II y las apreciaciones que luego se efectuarán, se trata de un requisito que, si no absolutamente decisivo, en la práctica judicial sí se considera de enorme importancia para apreciar que la inspección empresarial resulta respetuosa con los derechos fundamentales de las personas trabajadoras[17].

3.2. Alcance en el control mediante geolocalización

Frente a la regulación minimalista –o cuando menos, ambigua– del requisito de información previa en los dispositivos digitales, en el extremo opuesto se sitúa la regulación dada por la LOPD respecto a la admitida posibilidad de control laboral mediante geolocalización.

a) En este caso, el art. 90.2 LOPD sí impone explícitamente a la empresa que, de forma expresa, clara e inequívoca, informe con carácter "previo" a los trabajadores y sus representantes respecto a "la existencia y características" de los geolocalizadores, debiendo indicarles también el posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. Además, aun cuando esta cuestión también ha sido foco de conflicto[18], considero que, pese a no explicitarse en el precepto, esa infor-

[16] De acuerdo con su "Guía para el cumplimiento del deber de informar" de 2018, si los datos se obtienen del interesado, la información se le debe facilitar "en el momento en que se soliciten los datos, previamente a la recogida o registro".

[17] STS de 8 de febrero de 2018 (Rº. 1121/2015, Sala de lo Social); SSTSJ de Andalucía/Granada, de 21 de enero de 2021 (Rº. 1411/2020); Madrid, de 30 de junio de 2021 (Rº. 428/2021).

[18] En favor de que el tenor del art. 90.2 LOPD no impone informar a los trabajadores sobre la finalidad de control laboral de los dispositivos de geolocalización, *vid.* AGUILERA IZQUIERDO, R., "El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización", *Revista de Trabajo y Seguridad Social. CEF* nº 442, 2020, pp. 130-131; FERNÁNDEZ FERNÁNDEZ, R., "La geolocalización como mecanismo de control laboral: alcance y límites de una controvertida herramienta del poder directivo", *Revista de Trabajo y Seguridad Social. CEF* nº 452, 2020, pp. 37-38.

mación debe incluir todas las menciones exigidas por la normativa general de protección de datos (art. 11 LOPD y arts. 13 y 14 Reglamento [UE] 2016/679)[19]. Por tanto, ello supone que, entre otras indicaciones, también aquí la empresa debe precisar la finalidad a la que va a destinarse ese tratamiento de datos obtenidos mediante los dispositivos de geolocalización –en su caso, su utilización con fines de control laboral *ex* art. 20.3 ET–, rigiendo igualmente el indicado principio de limitación de la finalidad[20].

En definitiva, de lo dicho se infiere que, con relación a la geolocalización, el art. 90.2 LOPD impone al empresario una información previa y completa, que además se establece con carácter absoluto, pues el precepto no prevé ningún supuesto de excepción o atenuación –ni siquiera contempla la del hallazgo casual, que, como luego se verá, sí se admite en el caso de la videovigilancia–.

b) A partir de las anteriores afirmaciones cabe plantearse si, ante ese nuevo régimen legal, es posible seguir aplicando el criterio jurisprudencial que, con relación a hechos anteriores a la LOPD, ha mantenido el Tribunal Supremo en materia de geolocalización.

En concreto, en su STS de 15 de septiembre de 2020 (R.º 528/2018, Sala de lo Social) se enjuició el supuesto de una trabajadora a la que la empresa había facilitado un vehículo para utilizarlo exclusivamente durante la jornada laboral. La empresa le había informado de que el vehículo tenía instalado un geolocalizador, indicándole que su finalidad era la de "garantizar la seguridad y coordinación de los trabajos". Sin embargo, con posterioridad, ese dispositivo de geolocalización permitió a la empresa constatar que el vehículo era usado fuera de la jornada laboral e incluso en períodos de baja por incapacidad temporal, de modo que, como consecuencia de esta constatación, se procedió al despido de la trabajadora. Pues bien, pese a que finalmente el geolocalizador instalado fue usado con tales fines disciplinarios, el Tribunal Supremo corrige el criterio de la sentencia de suplicación y aprecia la validez de la prueba aportada por la empresa[21].

Respecto a esta decisión judicial, en el plano estrictamente legal cabría valorar la adecuación de la decisión empresarial al comentado principio de limitación de la

[19] *Vid.* BAZ RODRÍGUEZ, J., "La Ley…", cit., pp. 23-24; ALEGRE NUENO, M., "La utilización de sistemas de geolocalización para controlar la actividad laboral", en TALÉNS VISCONTI, E.E. y VALLS GENOVARD, M.A. (Dir.), *La actividad de los detectives privados en el ámbito laboral. Aspectos sustantivos y procesales de la obtención de la prueba*, Bosch Wolters Kluwer, Madrid, 2020, pp. 182-186.

[20] *Vid.* SERRANO OLIVARES, R., "Los derechos…", cit., p. 225; RODRÍGUEZ CARDO, I.A., "Utilización de sistemas de geolocalización en el ámbito laboral", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021, pp. 294, 301-302.

[21] Según indica el Tribunal Supremo, "No podemos compartir las conclusiones de la sentencia recurrida respecto de que ese control excede a la finalidad del dispositivo de localización. La seguridad del vehículo –y la responsabilidad civil que pudiera aparejarse de un quebranto de la misma– sigue hallándose en la esfera de las obligaciones de la empresa, como titular del mismo, fuera de la jornada de trabajo. […] En suma, la trabajadora conocía que el vehículo no podía ser utilizado fuera de la jornada laboral y, junto a ello, que el mismo estaba localizable a través del receptor GPS. De ahí que no apreciamos ninguna invasión en sus derechos fundamentales con la constatación de los datos de geolocalización que permiten ver que el indicado vehículo es utilizado desobedeciendo las instrucciones de la empresa en momentos en que no existía prestación de servicios. Había conocimiento previo y no se aprecia invasión de la esfera privada de la trabajadora, al afectar exclusivamente a la ubicación y movimiento del vehículo…".

finalidad del tratamiento de datos, pudiendo plantearse, por lo antes dicho, si los fines informados son compatibles con la finalidad de control y consiguientes efectos sancionadores posteriormente aplicados. Si tal adecuación ya podía ser puesta en cuestión bajo la normativa previa, con mayor razón ahora, contando ya con una regulación específica para las relaciones laborales, cabe preguntarse si esa separación de la finalidad informada resulta realmente conforme al régimen legal establecido por el art. 90 LOPD, que, como se ha dicho, no ha dispuesto ninguna atenuación respecto a las exigencias vinculadas al requisito de información previa[22].

Ahora bien, como antes se avanzaba, otra cosa es que nos situemos en el plano constitucional y nos planteemos si ese eventual incumplimiento legal –en este caso, una desviación de la finalidad informada– va a determinar en todo caso que el control empresarial se considere lesivo de los derechos fundamentales de los trabajadores o si, por el contrario, todavía habría posibilidad de apreciar su legitimidad, como sucede en la Sentencia referida.

Esta última es una cuestión que, aun en relación con otro medio de control distinto –grabaciones de audio– y también en el contexto de la normativa previa, subyacía en un supuesto recientemente enjuiciado por la STC 160/2021, de 4 de octubre, en el que asimismo se alegaba que ese instrumento –y el consiguiente tratamiento de datos– había sido utilizado con unos fines disciplinarios de despido, distintos a los que inicialmente se habían comunicado e incluso pactado con los representantes de los trabajadores[23]. Al amparo de los hechos, sin embargo, el Tribunal Constitucional evita abordar esta cuestión[24], por lo que, de momento, nos hemos quedado sin conocer su actual criterio

[22] Respecto a hechos acaecidos ya bajo la vigencia de la LOPD, las SSTSJ de Cataluña, de 28 de octubre de 2020 (Rº. 1354/2020); Madrid, de 21 de abril de 2021 (Rº. 144/2021), han dado validez a la prueba obtenida de dispositivos de geolocalización a efectos de acreditar decisiones empresariales disciplinarias, en supuestos en que constaba que la persona trabajadora había sido informada de su utilización con fines de control laboral. Desde otra óptica, la STSJ de Cataluña de 17 de febrero de 2021 (Rº. 4700/2020) considera aplicable analógicamente la atenuación establecida en el art. 89.1 LOPD para supuestos de captación de comisión flagrante de acto ilícito, y en un caso en que sí había mediado información previa al trabajador de la instalación del dispositivo de geolocalización, admite en tales situaciones un menor rigor en el deber de información.

Por su parte, la Resolución de la AEPD de 24 de septiembre de 2020, en el procedimiento PS/00124/2019, relativo a un empleado municipal, considera vulnerado el art. 5.1.b) Reglamento [UE] 2016/679, por cuanto los datos de geolocalización se utilizaron con fines de control laboral cuando se habían informado para fines de gestión y coordinación de patrullas y agentes.

[23] En este supuesto enjuiciado en la STC 160/2021, si bien los trabajadores –asesores comerciales telefónicos– habían sido informados de que sus conversaciones con los clientes podían ser objeto de grabación, constaba un acuerdo con los representantes de los trabajadores en que la empresa había pactado que dichas grabaciones sólo tenían como fin detectar insuficiencias de los empleados al objeto de proporcionarles la formación necesaria, pero que en ningún caso se utilizarían con fines disciplinarios. Sin embargo, constatadas ciertas deficiencias en la prestación de uno de los trabajadores a través de estas grabaciones, la empresa le facilitó indicaciones sobre el modo en que debía realizar el trabajo, pero, no apreciando mejora, finalmente le despidió.

[24] Habiendo alegado el trabajador vulneración de su derecho a la protección de datos personales, esta STC 160/2021 desestima el amparo por considerar que las grabaciones sí se habían utilizado inicialmente con los

respecto a la incidencia que un uso desviado de la finalidad informada tiene sobre el respeto al derecho de protección de datos personales y, en definitiva, sobre la validez de la actuación empresarial[25].

Nos encontramos, por tanto, ante un interrogante abierto, sobre el que en breve volveremos. Previamente, interesa concluir el régimen legal que en materia de información previa ha establecido la LOPD respecto al último instrumento de control que resta por analizar –la videovigilancia–.

3.3. Alcance en el control mediante videovigilancia

Entre la exigencia indefinida o difusa en los dispositivos digitales y la máxima en la geolocalización, la regulación legal de la información previa respecto a la instalación de la videovigilancia se sitúa en una posición intermedia, por la vía de diferenciar en el art. 89.1 LOPD dos supuestos distintos, con niveles de imposición diferentes.

a) Por un lado, en su primer párrafo, el precepto regula la instalación de cámaras con fines de control laboral *ex* art. 20.3 ET[26]. Cuando se trata de la grabación de imáge-

---

fines de calidad y formación anunciados y que, en realidad, el despido se había producido por la persistente renuencia del trabajador a cumplir las indicaciones empresariales, de ahí que, según la Sentencia, la determinación de si esta sanción es o no compatible con el pacto alcanzado constituía una cuestión que ya era ajena al contenido del derecho fundamental. Tal es la respuesta del Tribunal Constitucional, pese a que, inicialmente, la especial transcendencia constitucional apreciada para admitir el recurso de amparo había sido la de "determinar la relevancia que para la configuración del derecho a la protección de datos del carácter personal (artículo 18.4 CE) tienen las condiciones pactadas entre las partes respecto del uso de los datos de carácter personal obtenidos mediante estas grabaciones". Tampoco explica la fundamentación cómo se constató la reiteración de incumplimientos del trabajador.

Un comentario de esta Sentencia, con referencia al uso opuesto al informado realizado por la empresa y la posible vulneración de los arts. 5 y 6.4 Reglamento [UE] 2016/679, puede verse en MOLINA NAVARRETE, C., "Eficacia de gestión versus protección de datos: ¿reactividad jurisdiccional a la «inflación de derechos humanos» (en el trabajo)? Comentario a la Sentencia del Tribunal Constitucional 160/2021, de 4 de octubre", *Revista de Trabajo y Seguridad Social. CEF* nº 465, 2021, pp. 109-122. También, *vid.* MERCADER UGUINA, J.R., "Nuevas señales y paradojas de la protección de datos en la reciente doctrina de los Tribunales y de la Agencia Española de Protección de Datos", *Trabajo y Derecho* nº 85/2022, smarteca, pp. 20-21.

[25] Como ya se ha visto en una nota previa, recordemos que, respecto a la información de la finalidad del tratamiento de datos, la jurisprudencia constitucional previa había mostrado disparidad de criterios en las SSTC 29/2013 y 39/2016.

[26] Sobre la admisión legal de esta finalidad, ALTÉS TÁRREGA, J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda II", *Revista General de Derecho del Trabajo y de la Seguridad Social* nº 55, 2020, pp. 335 y ss; LAHERA FORTEZA, J., "Videovigilancia laboral y grabación de sonidos en el lugar de trabajo", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021, p. 266. *Vid.* asimismo la sistematización de supuestos previstos en el art. 89.1 LOPD que realiza la STSJ de Galicia, de 15 de febrero de 2021 (Rº. 4586/2020).

En cambio, una posición más restrictiva mantiene BAZ RODRÍGUEZ, J., "La Ley…", cit., pp. 13-14, para quien "el artículo 89 LOPDP-GDD no ha venido, desde luego, a legitimar el control directo de la actividad laboral a través de técnicas de videovigilancia, sino únicamente a establecer límites al control indirecto de la misma que se pueda derivar de establecimiento de medidas de videovigilancia justificadas en atención a la exclusiva finalidad de proteger la seguridad de las personas, bienes e instalaciones existentes en la empresa".

nes[27], esta es una posibilidad expresamente admitida por la norma[28]. Cierto es que, cuanto más nos alejemos de fines de seguridad, más dificultades tendrá la empresa para justificar la medida de control y superar el principio de proporcionalidad[29], dado que, en atención a esta exigencia, no podemos convertir los centros de trabajo en ámbitos abiertos a la libre e indiscriminada grabación continua[30]. Como siempre, habrá que valorar en cada caso la adecuación de la medida empresarial. Pero si finalmente se instalan estas cámaras, lo que sí impone el art. 89.1 LOPD a las empresas es que, de forma expresa, clara y concisa, proporcionen información "previa" a los trabajadores y sus representantes "acerca de esta medida". Pese a la ambigüedad de esta última expresión –a diferencia del art. 90.1 LODP, ni siquiera alude a "la existencia y características" del dispositivo–, también aquí considero que, en este primer supuesto, se requiere una información completa, con las exigencias requeridas por la normativa general de protección de datos, incluida la referencia a la finalidad del tratamiento, lo que en este caso implica indicar que la videovigilancia está dirigida al control laboral, con los posibles efectos sancionadores que pueden derivar[31].

Esta es una importante diferencia respecto al segundo supuesto contemplado en el segundo párrafo del art. 89.1 LOPD, referido a los casos en que las empresas instalan cámaras de videovigilancia con fines de seguridad, esto es, dirigidas a preservar las personas, bienes e instalaciones. De acuerdo con la normativa general, para entender cumplido el requisito de información respecto a este tipo de videovigilancia basta con colocar en un lugar visible el dispositivo general que anuncia la existencia de cámaras –esto es,

---

[27] Obsérvese la diferencia de redacción con el art. 89.3 LOPD, que respecto a la grabación de sonidos en el lugar de trabajo indica que "se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo…".

[28] Ahora bien, de acuerdo con el art. 89.2 LOPD, "en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos".

Al respecto, STC 98/2000, de 10 de abril, FJ 6; y STEDH López Ribalda II. En la doctrina judicial interna posterior a la LOPD, STSJ de I. Canarias/Las Palmas, de 23 de junio de 2021 (Rº. 600/2021), que considera lesiva de los derechos fundamentales una cámara que capta "un cuartito" destinado por los trabajadores a "desayunar, agua, botiquín"; y la misma solución, entre otras, SSTSJ de I. Canarias/Las Palmas, de 8 de marzo de 2021 (Rº. 967/2020); o de 28 de septiembre de 2021 (Rº. 971/2021), respecto a cámara que graba "además del aparato del sistema de control horario, parte del comedor del personal y la zona de entrada a los vestuarios".

[29] ALTÉS TÁRREGA, J.A., "La videovigilancia…", cit., pp. 336 y 340.

[30] *Vid.* MERCADER UGUINA, J.R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Francis Lefebvre, Madrid, 2019, 3ª ed., p. 139, quien en tal sentido recuerda el criterio de la SAN de 24 de enero de 2003 (Rº. 400/2001, Sala de lo Contencioso-administrativo); GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I.A., "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo* nº 216, 2019, BIB 2019\1432, p. 39.

[31] *Vid.* ALTÉS TÁRREGA, J.A., "La videovigilancia…", cit., pp. 332 y 343; MOLINA NAVARRETE, C., "Régimen legal de los sistemas de control laboral basados en la videovigilancia: lagunas y antinomias a la luz del Derecho Comunitario", en RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A. (Dir.), *Vigilancia y control en el Derecho del Trabajo Digital*, Aranzadi, 2020, pp. 79 a 81; LAHERA FORTEZA, J., "Videovigilancia…", cit., p. 269.

el conocido cartel regulado en el art. 3 de la Instrucción 1/2006, de la AEPD–, con la minoración en el contenido que dispone el art. 22.4 LOPD, que sólo impone identificar "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", aun cuando el precepto legal exige además tener a disposición de los afectados la información requerida por el citado Reglamento comunitario[32]. Pues bien, en el ámbito laboral, lo que aporta el segundo párrafo del art. 89.1 LOPD es que, existiendo dicho distintivo, la exigencia de información se entenderá igualmente cumplida cuando a través de esas cámaras instaladas con fines de seguridad se capta la "comisión flagrante de un acto ilícito" por los trabajadores. Es lo que se conoce como las situaciones de "hallazgo casual", aunque, a mi juicio, ese carácter "casual" resulta a menudo bastante cuestionable en la práctica. No obstante, es la expresión con la que normalmente se alude a estos supuestos respecto a los que ahora la LOPD admite, no una eliminación, pero sí una atenuación o modulación en cuanto a las exigencias del requisito de información previa, dado que se permite constatar y acreditar ilícitos laborales, con posibles efectos disciplinarios, pese a que inicialmente la instalación de cámaras se informó con la mera colocación del dispositivo informativo y con fines exclusivos de seguridad.

b) Este segundo supuesto en que la propia ley admite una información atenuada o modulada es, sin duda, el que más interrogantes interpretativos plantea.

Uno de ellos es el de concretar el alcance "espacial" del dispositivo informativo a efectos de dispensar de la información completa o específica. Así, por ejemplo, si a la entrada de un centro de trabajo se coloca el cartel informativo de videovigilancia, cabe preguntarse a qué dependencias –todas o algunas– se extiende la posibilidad de considerar cumplido el requisito de información previa en caso de constatar en ellas un ilícito laboral. Esta cuestión se ha planteado en algún pronunciamiento judicial, como la STSJ Galicia de 15 de febrero de 2021 (Rº. 4586/2020), en la que viene a afirmarse que la eficacia del dispositivo informativo debe quedar limitada al espacio al que se accede desde la visualización del cartel, sin extenderse a otras dependencias cerradas y separadas[33].

[32] Con relación a esta última exigencia del art. 22.4 LOPD, la Resolución de la AEPD de 17 de enero de 2022, dictada en el procedimiento PS-00479-2021, ha afirmado: "cabe señalar que el resto de las cuestiones contempladas en el artículo 13 del RGPD «deben mantenerse a disposición de los afectados», esto es, en un lugar al que pueda acceder fácilmente el interesado".

[33] Afirma esta Sentencia: "Aquí se plantea la cuestión de si los dispositivos informativos contenidos en una cámara de seguridad generalista … tienen eficacia en todo el centro de trabajo, a lo que, a juicio de la Sala, solo podríamos dar una respuesta afirmativa si existiera una continuidad entre todos los espacios a los cuales se puede acceder desde la visualización del dispositivo informativo. Por ello, la información contemplada en el dispositivo informativo de una cámara generalista entendemos no es efectiva en espacios diferenciados como los del supuesto de estos autos (espacios cerrados, separados del resto de espacios donde estaban las cámaras de seguridad hasta entonces instaladas, sin acceso al público, e incluso con acceso limitado al personal de la empresa)".

Por su parte, la Sentencia del Juzgado de lo Social núm. 2 de Guadalajara de 24 de junio de 2021 (Procedimiento núm. 277/2021), declara nula la prueba de videovigilancia por considerar que la información dada no es clara y completa, alegando a tal efecto que "hay un cartel a la entrada de la empresa y ello puede dar lugar a pensar que la zona videovigilada es precisamente la zona de influencia de dicho cartel, a saber la

Ciertamente, sea este el criterio o uno análogo, parece razonable que un límite espacial ha de ponerse a la regla establecida en el párrafo segundo del art. 89.1 LOPD porque, de lo contrario, en ocasiones estaríamos convirtiendo el dispositivo informativo en una mera formalidad y no en una garantía efectiva, que es lo que debe ser[34].

c) En cualquier caso, más problemático puede resultar el alcance "objetivo" de esa regla de atenuación o modulación informativa establecida. Al margen de otras dificultades interpretativas referidas a la captación –caso del significado de comisión "flagrante"[35]–, interesa concretar el tipo de ilícitos laborales que, según el art. 89.1 LOPD, podrían entenderse válidamente constatados a través de estas cámaras instaladas con fines de seguridad. En el momento de elaborar este análisis no consta que por el momento existan pronunciamientos del Tribunal Supremo relativos a hechos acaecidos con posterioridad a la vigencia de la LOPD de 2018. Sí los hay, desde luego, respecto a situaciones producidas bajo la normativa previa, y en ellos se observa que el Tribunal Supremo ha venido haciendo una interpretación amplia del término "seguridad" y, por tanto, del valor informativo del cartel anunciador de las cámaras, con la consecuencia a su vez de hacer una lectura flexible respecto a los ilícitos laborales que pueden ser válidamente constatados por esta vía.

De un lado, el Tribunal Supremo ha considerado suficiente esa información no sólo para constatar la comisión por los trabajadores de actos delictivos (*v.gr.* supuestos de hurto o apropiaciones indebidas[36]), sino también de meros incumplimientos contractuales de menor alcance (*v.gr.* otros actos de transgresión de la buena fe o de negligencia

recepción, pero no es extensiva tal información a la zona de trabajo, en la que desconocemos… que existan también carteles que informen acerca de que dichas instalaciones, completamente independientes de la recepción, también estén videovigiladas".

[34] Es cierto que, de acuerdo con el Informe 0084/2007 de la AEPD, "respecto de la ubicación del cartel informativo, no es necesario que se coloque debajo de la cámara, será suficiente conforme a lo dispuesto en el artículo 3 a) de la citada Instrucción, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por tanto, resultaría aconsejable que si tratándose de un edificio sometido a videovigilancia, en la entrada del mismo, se ubicará el cartel informativo". Ahora bien, conforme a las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, acordadas por el Comité Europeo de Protección de Datos (versión de 29 de enero de 2020), cuando se coloca la señal de advertencia no es necesario revelar la posición de la cámara, pero "siempre y cuando no haya dudas respecto a las zonas sujetas a vigilancia y el contexto de esta quede claro de forma inequívoca (WP 89, apartado 22). El interesado debe poder estimar qué zona se captura por una cámara de forma que pueda evitar la vigilancia o adaptar su comportamiento si fuera necesario".

[35] *Vid.* LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., "Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral", en MONREAL BRINGSVAERD, E., THIBAULT ARANDA, X., JURADO SEGOVIA, A., *Derecho del trabajo y nuevas tecnologías*, Tirant lo blanch, Valencia, 2020, p. 414, para quienes, como ilícitos cometidos de manera flagrante, admiten tanto los captados de manera sorpresiva –sin sospecha previa–, como los constatados tras un control más específico realizado a partir de fundadas sospechas. En cambio, LAHERA FORTEZA, J., "Videovigilancia…", cit., pp. 273 y 274, afirma que "si la comisión es flagrante es que no había indicios previos de dicha acción grabada", si bien, después alude a esta previsión para proponer una posible admisión de cámaras ocultas ante indicios previos de irregularidades graves.

[36] STS de 31 de enero de 2017 (Rº. 3331/2015, Sala de lo Social), respecto a manipulación de tickets y hurto de cantidades por un trabajador.

en el trabajo[37]). Tal criterio podría seguir teniendo cabida en el segundo párrafo del art. 89.1 LOPD, que a la vista de su tenor y de su tramitación parlamentaria, se refiere a *actos ilícitos*, sin explícita exigencia de su naturaleza penal[38].

Pero, además, de otro lado, parece que el Tribunal Supremo ha pasado a considerar que esa información atenuada es suficiente incluso para constatar ilícitos laborales no estrictamente vinculados a fines de seguridad de las personas y cosas, apreciándose en este aspecto una cierta evolución expansiva en su jurisprudencia. Al respecto recordemos que la STC 39/2016, de 3 de marzo, había afirmado que, existiendo el cartel informativo de las cámaras de seguridad, no hacía falta especificar "la finalidad exacta" de control sobre los trabajadores, si bien es cierto que en aquel caso se enjuiciaba la constatación de un ilícito laboral –unas apropiaciones dinerarias– vinculado a tal objetivo. Pues bien, incluso tras esta Sentencia constitucional, algunos pronunciamientos del Tribunal Supremo emitidos en 2017 advirtieron que las cámaras de seguridad excluían el control sobre ilícitos laborales ajenos a dicha finalidad de seguridad (*v.gr.* efectividad en el trabajo, ausencias, conversaciones con compañeros, etc)[39]. Sin embargo, frente a este criterio más restrictivo, con posterioridad y sobre todo en el año 2021, se han dictado otros pronunciamientos en que parece haberse ampliado el criterio, admitiendo como lícito el control empresarial realizado con cámaras de seguridad respecto a incumplimientos laborales no directamente ligados a la seguridad en la empresa, al menos en sentido estricto[40].

Uno de estos pronunciamientos, dictado en la Sala de lo Social, es la STS de 13 de octubre de 2021 (Rº. 3715/2018), en la que se ha afirmado expresamente que la justificación de cámaras de vigilancia por razones de seguridad en sentido amplio "incluye el control de la actividad laboral". A partir de este presupuesto, el Tribunal Supremo admite como lícita la prueba de videovigilancia aportada por la empresa en un supuesto en que, pese a que se había informado al conductor de un autobús sobre la existencia de una cámara con fines de seguridad, después las grabaciones se utilizan para despedirle disciplinariamente porque a través de ellas se constatan determinados ilícitos laborales, en principio no vinculados de forma inmediata a esa finalidad, como no cobrar el billete

[37] STS de 21 de julio de 2021 (Rº. 4877/2018, Sala de lo Social), relativa a un vigilante de seguridad en un recinto ferial, a quien, por haberse incrementado la alerta por amenaza terrorista, se le había ordenado la inspección de los vehículos que entraban, orden que las cámaras de seguridad del recinto mostraron que no cumplía, pese a que en los partes diarios reflejaba los controles como realizados.

[38] *Vid.* STSJ Galicia de 15 de febrero de 2021 (Rº. 4586/2020); SERRANO OLIVARES, R., "Los derechos…", cit., p. 223; LAHERA FORTEZA, J., "Videovigilancia…", cit., p. 272.

[39] STS de 31 de enero de 2017 (Rº. 3331/2015, Sala de lo Social): "…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. etc..". También, STS de 1 de febrero de 2017 (Rº. 3262/2015, Sala de lo Social).

[40] Previamente a los que arriba se citan, la STS de 2 de febrero de 2017 (Rº. 554/2016, Sala de lo Social), otorgó validez a la prueba videográfica para dar por acreditados determinados incumplimientos laborales de un trabajador, sólo parcialmente relacionados con fines de seguridad: no sólo haber permitido el acceso gratuito a las instalaciones de un gimnasio a personas no autorizadas, sino también incumplimientos de jornada.

a una pasajera o realizar determinadas conductas en su período de descanso entre rutas, como tocamientos y caricias a aquélla, fumar en el autobús u orinar desde el mismo.

Más clara incluso puede ser la STS de 26 de abril de 2021 (Rº. 4645/2019), en este caso dictada por la Sala de lo Contencioso-Administrativo. En ella también se da validez a la prueba de videovigilancia aportada por una Administración para justificar la sanción disciplinaria impuesta a una funcionaria porque, a través de cámaras instaladas con fines de seguridad, se habían constatado diversas acciones dirigidas a burlar los mecanismos de control horario.

Como vemos, se trata de pronunciamientos recientes del Tribunal Supremo, dictados bajo la vigencia de la normativa previa, en que el uso de las cámaras de seguridad se considera válido para legitimar decisiones empresariales disciplinarias respecto a ilícitos laborales no estrictamente vinculados a preservar las personas y las cosas. En consecuencia, de cara a futuros pronunciamientos, también aquí cabe preguntarse por la valoración que merece la aplicación de este criterio a la luz de la nueva normativa implantada por la LOPD de 2018.

Si nos situamos en el plano de la estricta legalidad, a mi juicio cabría entender que si se sigue haciendo una interpretación amplia del término "seguridad" y si se estira mucho la regla excepcional de información atenuada del segundo párrafo del art. 89.1 LOPD, al final estaríamos dejando en papel mojado la regla general de su párrafo primero, que, como hemos visto, cuando se trata de la instalación de cámaras de videovigilancia con fines de control laboral impone la exigencia de información plena y expresa, además de que, como se ha advertido, su admisión puede ser mucho más limitada por resultar más difícil acreditar su justificación y proporcionalidad. Es cierto que, pese a existir opiniones favorables a que esta previsión legal contraviene el Reglamento [UE] 2016/679[41], no creo que esta deba ser necesariamente la conclusión, siempre que, en su interpretación, se busque la conexión entre los supuestos de aplicación de la regla atenuada y la finalidad informada de seguridad –ello, claro está, a menos que se cuestione la propia adecuación del art. 22.4 LOPD[42]–. Sin embargo, respecto a los ilícitos laborales constatados, sí entiendo que cuanto más se alejen de ese fin de seguridad, más dudas pueden generarse, no sólo en cuanto a la adecuación a esa normativa general de protec-

[41] *Vid.* Sentencia del Juzgado de lo Social núm. 3 de Pamplona de 18 de febrero de 2021 (Procedimiento núm. 754/2020), que, con relación a la acreditación de una conducta de acoso sexual mediante la grabación de cámaras de seguridad anunciadas mediante cartel, razona que el Reglamento [UE] 2016/679 no contempla excepciones en cuanto a las exigencias del deber de información de la finalidad, y en consecuencia, partiendo de que esta norma comunitaria es vulnerada por el art. 89.1 LOPD, procede a la inaplicación de esta previsión interna y declara la nulidad de la prueba. Previamente, respecto a hechos anteriores a la LO. 3/2018, Sentencia del Juzgado de lo Social núm. 3 de Pamplona de 18 de febrero de 2019 (Procedimiento núm. 875/2018). En línea similar, *vid.* MOLINA NAVARRETE, C., "Régimen…", cit., pp. 90 a 92.

[42] Recordemos que el art. 22.4 LOPD no exige que en el dispositivo informativo se indiquen los fines del tratamiento –previamente, el apartado 1 del precepto vincula las videocámaras a "la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones"–, pero sí impone que "en todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento *[Reglamento (UE) 2016/679]*".

ción de datos, sino también respecto a la propia coherencia interna del art. 89.1 LOPD, que, por lo dicho, requeriría una interpretación restrictiva de su párrafo segundo[43], en línea con la lectura que algunos pronunciamientos de la doctrina judicial reciente vienen reflejando[44]. Obsérvese, además, que el art. 42.4 de la Ley 5/2014, de Seguridad Privada, continúa afirmando que "las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad".

Cuestión diferente nuevamente es plantearnos si, desde el plano constitucional, la omisión de esa información plena y expresa cuando ésta proceda habría de llevar en todo caso a considerar vulnerados los derechos fundamentales de los trabajadores o si, por el contrario, habría aún posibilidad de admitir la validez de la prueba empresarial. Pues bien, una vez expuesto el régimen legal, procede ya, por fin, adentrarse en la resolución de este interrogante que se ha venido abriendo en sucesivos subepígrafes.

[43] Sobre la vinculación entre el supuesto del párrafo 2º del art. 89.1 LOPD y los ilícitos laborales vinculados al deber de seguridad y protección de las personas y las cosas, *vid.* LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., "Derecho…", cit., pp. 411-413 y 417.

[44] La STSJ de Galicia, de 16 de enero de 2020 (Rº. 5278/2019), admite la validez de la prueba de videovigilancia, entre otras razones, porque el incumplimiento imputado a la trabajadora "no se refiere a las obligaciones vinculadas a la prestación laboral –cumplimiento de horario, exigencia de rendimiento, ausencias al trabajo, distracciones en el trabajo...–, sino a una flagrante sustracción de documentos, siendo oportuno recordar que la precisión de contenidos tiene diferente alcance cuando se trata de incumplimientos laborales, u otros vinculados con la seguridad". Asimismo, la STSJ de Asturias, de 27 de abril de 2021 (Rº. 243/2021), niega validez a la prueba de videovigilancia para acreditar determinados ilícitos laborales –*v.gr.* desatención a clientes, fumar y beber en el lugar de trabajo, sustracción de documentos confidenciales, abandono del puesto de trabajo…–, por cuanto que "hay una notable diferencia entre el conocimiento de la existencia de cámaras en el contexto y para la finalidad que fueron instaladas –prevención de ilícitos por terceros esencialmente– y la concreta utilización que nos ocupa de manera prospectiva y retroactiva para fines de control empresarial del eventual incumplimiento de obligaciones laborales respecto de las que no existía la mínima tacha o sospecha". De forma similar, la STSJ de Cataluña, de 29 de julio de 2021 (Rº. 1993/2021), también considera ilegítima la prueba de videovigilancia, dado que, si bien existían carteles de zona de videovigilancia con fines de seguridad, no se había informado del potencial uso de las imágenes para control laboral, remarcándose, además, que en el caso no existían sospechas concretas de incumplimiento laboral; o en una línea similar, STSJ de Cataluña, de 18 de enero de 2021 (Rº. 3892/2020); o Sentencia del Juzgado de lo Social núm. 1 de Oviedo de 14 de julio de 2020 (Procedimiento núm. 49/2020). Incluso respecto a la imputación de unas apropiaciones indebidas, la STSJ de País Vasco, de 6 de octubre de 2020 (Rº. 956/2020), considera ilegítima la prueba captada con cámaras de seguridad por no haber informado a los trabajadores de que también podían utilizarse para el control de su actividad y entender que no se trataba de una situación excepcional dado que la empresa ya había utilizado el mismo medio en el despido previo de otro trabajador; y también Sentencias de los Juzgados de lo Social núm. 1 de Zamora de 26 de marzo de 2021 (Procedimiento núm. 240/2020); o núm. 5 de Palma de Mallorca de 12 de julio de 2021 (Procedimiento núm. 828/2020).

Por su parte, con apoyo en la STC 39/2016, la SAN de 30 de noviembre de 2021 (Rº. 226/2021) recupera la idea de que, cuando el trabajador conoce que se ha instalado un sistema de videovigilancia, no es obligado especificar "la finalidad exacta que se le ha asignado a ese control", si bien lo hace en un supuesto en que la inspección empresarial se efectúa con fines de seguridad, y además, la medida –registro de bolsos ante las cámaras como control preventivo, sin sospechas previas de hurtos– se declara nula por no superar el principio de proporcionalidad, valorándose en la ponderación, entre otros aspectos, que no se haya informado a los trabajadores sobre la recogida de datos, su objeto y finalidad.

4. Incumplimientos del deber de información: ¿ilegalidad e inconstitucionalidad?

En efecto, el objeto de este último apartado del análisis es el de tratar de determinar las consecuencias de los incumplimientos relativos a los requisitos legales de información en el tratamiento de datos personales cuando se producen en el marco del control tecnológico laboral.

Como primera consecuencia, es evidente que estas infracciones pueden generar la responsabilidad administrativa de la empresa, bien ante la autoridad de protección de datos o bien ante la autoridad laboral. Pero la cuestión es si, además, esos incumplimientos de las exigencias legales de información van también a provocar en todo caso la nulidad de la prueba por lesión de derechos fundamentales.

Si volvemos a los dos elementos que configuran el canon de enjuiciamiento del control empresarial, no hay ninguna duda de que el principio de proporcionalidad siempre debe superarse para poder entender que la vigilancia empresarial es válida[45]. La duda se plantea respecto a si la presencia del segundo elemento –el relativo a la información previa– es también indispensable para admitir el carácter legítimo de la medida empresarial.

a) Si acudimos de nuevo a la jurisprudencia europea resulta que, pese a lo que inicialmente pudiera inferirse de la STEDH Bărbulescu II, de pronunciamientos posteriores del Tribunal Europeo de Derechos Humanos parece deducirse que el cumplimiento de las exigencias de información previa no es absolutamente imprescindible para admitir la validez del control empresarial. Así pareció apuntarse en la STEDH de 22 de febrero de 2018, dictada en el asunto Libert, en un supuesto de monitorización de ordenadores[46]. Pero, más claramente, esta es la conclusión que se extrae de la ya citada STEDH López Ribalda II de 2019, que, recordemos, se refería a un supuesto en que la empresa sí había informado previamente sobre unas cámaras visibles anunciadas con el correspondiente cartel, pero, en cambio, había omitido toda información respecto a unas cámaras ocultas, cuyas grabaciones, sin embargo, no se consideraron lesivas de los derechos de los trabajadores. Expresamente el Tribunal Europeo señaló que el requisito de información previa es sólo uno más de los ítems o garantías a ponderar en el enjuiciamiento del control empresarial y que su incumplimiento no determinaba en todo caso la nulidad de la fiscalización. Ahora bien, esta afirmación de la Sentencia venía también acompañada de dos matices: el primero es que, en aquellos casos en que se haya inobservado la exigencia de información previa, el Tribunal requiere que la aplicación del juicio de proporcionalidad ha de ser más rigurosa; y la segunda matización hecha por el Tribunal Europeo es

[45] Con relación a hechos posteriores a la LOPD, *v.gr.* SSTSJ de Cantabria, de 2 de noviembre de 2021 (Rº. 653/2021); Cataluña, de 26 de noviembre de 2021 (Rº. 4145/2021), respecto a videovigilancia.

[46] Esta Sentencia admite como legítima la inspección empresarial sobre unos archivos personales de un trabajador, a quien se había informado sobre el uso estrictamente profesional de tales medios –aun con admisión puntual de utilización privada–, pero sin constar que hubiera mediado previa advertencia específica sobre la posibilidad de controles empresariales. El TEDH justifica su decisión en que el trabajador no había identificado tales archivos como "privados" y en que, en el caso, la medida resultaba proporcionada al legítimo objetivo de protección de los intereses empresariales.

que esa ausencia del requisito informativo sólo podrá ser compatible con la validez del control empresarial de modo excepcional, de forma que la exigencia informativa sólo debe ceder ante imperativos importantes, que en el caso se concretaron en la existencia de sospechas "razonables" de irregularidades "graves" –en el supuesto se trataba de reiteradas sustracciones de mercancías por parte de varias personas trabajadoras–[47].

b) A la vista de esta jurisprudencia europea cabría pensar que, a nivel interno, la respuesta al interrogante antes formulado es clara y que no toda omisión del requisito de información previa, ya sea parcial o incluso total, convierte al control empresarial en ilegítimo. No obstante, ahora que ya contamos con un régimen legal específico para las relaciones laborales establecido en la LOPD de 2018, puede que la solución no sea tan sencilla. Al menos así resulta de la doctrina judicial emitida respecto a hechos posteriores a la Ley, pues han empezado a dictarse pronunciamientos que no mantienen un criterio unánime respecto al modo de proyectar esa jurisprudencia europea en nuestro ordenamiento.

El foco del conflicto reside en que, como hemos observado, al menos cuando se trata de videovigilancia y geolocalización, nuestra LOPD no establece ninguna excepción a la exigencia de información previa. A lo más que llega es a admitir el supuesto de información previa atenuada contemplado en el segundo párrafo de su art. 89.1, relativo a las cámaras de seguridad, pero en ningún momento la regulación legal hace mención a una omisión total del requisito. Precisamente, la existencia de ese régimen legal es el que ahora está dando lugar a resoluciones judiciales que no siguen las mismas pautas a la hora de abordar la inobservancia de este requisito legal.

Aunque el problema puede hacerse extensivo a los demás instrumentos de control, de momento la controversia judicial se está haciendo más visible en relación con las cámaras de videovigilancia ocultas respecto a las que ni siquiera se ha colocado el cartel o dispositivo general de información. En línea con lo dicho, en este caso el debate surge porque, si bien el art. 89 LOPD no prohíbe expresamente la instalación de cámaras ocultas, lo cierto es que es difícil encontrarles hueco o cobertura en el texto de esa regulación legal[48]. Pues bien, en este nuevo contexto normativo, es posible encontrar pronuncia-

[47] En palabras de la STEDH López Ribalda II, "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". A ello añade que "dada la importancia que tiene el derecho a la información en tales casos, el Tribunal considera que sólo un imperativo importante relativo a la protección de los intereses públicos o privados importantes podría justificar la ausencia de información previa", y "si bien no puede 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, la existencia de sospechas razonables de que se habían cometido graves irregularidades, y el alcance de los robos constatados en el presente asunto, pueden parecer una justificación seria".

[48] *Vid.* PÉREZ DE LOS COBOS ORIHUEL, F., "Poderes del empresario y derechos digitales del trabajador", *Trabajo y Derecho* nº 59/2019, smarteca, p. 10. En su opinión, "para asegurar la licitud del control, la obligación de información previa debiera en todo caso respetarse, bastando al efecto, eso sí, la colocación de etiquetas visibles que cumplan las exigencias legales". Por su parte, BAZ RODRÍGUEZ, J., "La Ley…", cit., pp. 18-20, considera que el art. 89.1 LOPD "no contempla una habilitación legal para la vigilancia total-

mientos de los Tribunales Superiores de Justicia que mantienen posiciones dispares respecto al modo de enjuiciar este tipo de videovigilancia encubierta.

Por un lado, algunas sentencias mantienen que, puesto que las cámaras ocultas no se encuentran admitidas por la LOPD, la prueba de videovigilancia debe considerarse lesiva de los derechos fundamentales de los trabajadores, llegándose a esta conclusión sin entrar a hacer una ponderación de las restantes circunstancias del caso[49] . En los supuestos enjuiciados, no se atiende a la dificultad reconocida de instalar el cartel informativo cuando se trata de trabajo doméstico, ni a la existencia de previas sospechas razonables de apropiaciones indebidas. Por el contrario, en estos pronunciamientos, el incumplimiento del régimen legal lleva como consecuencia inmediata la nulidad de la prueba de videovigilancia aportada por la empresa.

Frente a esta postura, en mayor medida encontramos otros pronunciamientos judiciales que, pese a partir de la vigencia y aplicación del régimen legal establecido en la LOPD de 2018, no niegan automáticamente la validez de la prueba obtenida de cámaras ocultas y, por el contrario, la decisión sobre su licitud o no se hace depender de si, tras la ponderación de las circunstancias del caso, se considera o no superado el principio de proporcionalidad[50].

c) Como se avanzaba, nos encontramos ante pronunciamientos contradictorios sobre las consecuencias del incumplimiento del régimen legal de la información previa, y aun cuando de momento la divergencia se está viendo respecto a la videovigilancia, ya he comentado que el conflicto podría trasladarse a los demás instrumentos de control. Es cierto que, como han propuesto algunos autores, la diligencia de las empresas podría evitar estos supuestos de omisión total de información previa y, como mecanismo intermedio en la salvaguarda de los derechos de las personas trabajadoras y la eficacia del control empresarial, podría cuando menos requerirse la existencia de una advertencia empresarial previa de que, ante la existencia de fundadas sospechas de irregularidades laborales graves, cabría la posibilidad futura de activar la instalación de dispositivos de vigilancia ocultos[51]. En la actualidad, sin embargo, la práctica judicial

---

mente secreta" y, además, propone interpretar que la atenuación informativa de su segundo párrafo requiere la previa existencia de sospechas fundadas de ilícitos.

[49] SSTSJ de Asturias, de 20 de octubre de 2020 (Rº. 1051/2020); Galicia, de 28 de junio de 2021 (Rº. 1545/2021). De forma más matizada, dado que también tiene en cuenta la doctrina de la STEDH López Ribalda II, *vid.* el razonamiento de STSJ de País Vasco, de 13 de octubre de 2020 (Rº. 1017/2020).

[50] SSTSJ de I. Canarias/Santa Cruz de Tenerife, de 1 de octubre de 2020 (Rº. 352/2020); Castilla-La Mancha, de 8 de febrero de 2021 (Rº. 1552/2020); Madrid, de 17 de febrero de 2021 (Rº. 819/2020); I. Canarias/Las Palmas, de 23 de junio de 2021 (Rº. 600/2021); Cataluña, de 18 de noviembre de 2021 (Rº. 4074/2021); Sentencia del Juzgado de lo Social núm. 1 de Zamora de 20 de septiembre de 2021 (Procedimiento núm. 239/2021). Asimismo, STSJ de Cataluña, de 11 de diciembre de 2020 (Rº. 4047/2020), que niega la legitimidad de la prueba por no existir sospechas previas del ilícito laboral constatado.

[51] *Vid.* PÉREZ DE LOS COBOS ORIHUEL, F., "Poderes…", cit., p. 10, quien afirma: "cabría pensar en la instalación de sistemas de videovigilancia focalizados sobre determinados puestos de trabajo, de cuya existencia el trabajador tuviera cumplida noticia, pero que solo serían objeto de activación –circunstancia que el trabajador debiera igualmente conocer– ante las fundadas sospechas de un comportamiento irregular". Por su parte, LAHERA FORTEZA, J., "Videovigilancia…", cit., p. 274, señala: "la aplicación de

expuesta muestra que son muchos los casos en que ni siquiera ha mediado este mínimo informativo.

Ante la disparidad de criterios en el enjuiciamiento de esos supuestos, habrá que esperar la solución unificadora del Tribunal Supremo o, en su caso, del Tribunal Constitucional. En todo caso, cierto es que, si atendemos a parámetros previos, la segunda postura judicial expuesta, que no equipara automáticamente infracción legal a infracción constitucional, cuenta con argumentos en su favor que, de una forma u otra, se reflejan en su fundamentación jurídica.

De una parte, dado el valor que, en virtud del art. 10.2 CE, alcanza la jurisprudencia europea en la interpretación interna de los derechos fundamentales, necesariamente ha de tenerse en cuenta la ya referida doctrina establecida en la STEDH dictada en el asunto López Ribalda II. Como apuntan los pronunciamientos de la primera postura, es verdad que, en el supuesto enjuiciado en esta Sentencia, la empresa al menos había informado y colocado el cartel informativo respecto a la existencia de las cámaras visibles. Sin embargo, no parece que esta circunstancia se haga valer en su argumentación para admitir la validez de las cámaras ocultas, pues, como antes se ha señalado, expresamente declara que la omisión del requisito de información previa no conduce en todo caso al carácter ilegítimo del control empresarial.

En cualquier caso, de otra parte, en la jurisprudencia constitucional interna, la STC 39/2016, dictada también en materia de videovigilancia, ya había asimismo apuntado que el incumplimiento del deber de información vinculado al derecho a la protección de datos no comporta necesariamente una vulneración del derecho, pues lo determinante es valorar en cada caso si se supera o no el juicio de proporcionalidad[52].

Este es el criterio clásico de nuestra jurisprudencia constitucional, que parte de que ningún derecho fundamental es absoluto y de que, en la colisión de bienes y derechos constitucionales, uno de ellos puede ser legítimamente limitado si tal sacrificio se considera proporcionado a partir de la ponderación de las circunstancias del caso[53]. En lo que ahora interesa, el mantenimiento de esta doctrina tras la LOPD llevaría a seguir concluyendo que no toda inobservancia del requisito de información previa es sinónimo de infracción constitucional, y que, por tanto, en determinados casos, el control empre-

transparencia del art.89.1.2º LOPD se puede hacer, en este tipo de cámara, con una información preventiva y previa de posible instalación de estos dispositivos ante hipotéticas y futuras sospechas de irregularidades del trabajador en el centro de trabajo".

[52] Respecto al deber de información, la STC 39/2016 señaló que "sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, en conexión con los arts. 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto".

[53] Por todas, SSTC 186/2000, FJ 5; o 128/2007, de 4 de junio, FJ 11.

sarial podría llegar a considerarse válido aunque no hubiera mediado un cumplimiento escrupuloso de tal exigencia[54].

En todo caso, como se ha dicho, a la vista de las primeras disensiones en la doctrina judicial, habrá que esperar a ver el peso que finalmente otorga nuestra jurisprudencia interna a la entrada en acción de la LOPD, y de este modo constatar si, en realidad, va a tener una incidencia significativa en ese criterio señalado. Ahora bien, de apostarse por su continuidad, sí me parece importante insistir en que, como indica la jurisprudencia europea, la admisión de la validez del control empresarial en supuestos de inobservancia total o parcial del requisito de información previa sólo debería admitirse de forma excepcional, cuando realmente existan imperativos relevantes que así lo justifiquen. Pues bien, desde esta perspectiva, considero que lo que quizá sí cabría repensar es la ponderación que a veces se observa en la práctica judicial interna, al objeto de que la aplicación de esta excepción, así como la de información atenuada *ex* art. 89.1 LOPD, se ajuste realmente a criterios restrictivos. Al fin y al cabo, ahora ya contamos con una regulación legal específica en el ámbito de las relaciones laborales; supuestamente, por tanto, las empresas tienen una mayor seguridad jurídica sobre lo que deben y pueden hacer; y lo que no tendría sentido es que, por la vía de hacer interpretaciones amplias de las excepciones, se acabara haciendo perder virtualidad a la Ley y a las garantías que con ella se han querido instaurar.

Bibliografía

AGUILERA IZQUIERDO, R., "El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización", *Revista de Trabajo y Seguridad Social. CEF* nº 442, 2020.

ALEGRE NUENO, M., "La utilización de sistemas de geolocalización para controlar la actividad laboral", en TALÉNS VISCONTI, E.E. y VALLS GENOVARD, M.A. (Dir.), *La actividad de los detectives privados en el ámbito laboral. Aspectos sustantivos y procesales de la obtención de la prueba*, Bosch Wolters Kluwer, Madrid, 2020.

ALTÉS TÁRREGA, J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda II", *Revista General de Derecho del Trabajo y de la Seguridad Social* nº 55, 2020.

BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho* nº 54/2019.

[54] Tras la LOPD, admiten la posible legitimidad del control empresarial mediante cámaras ocultas ante indicios previos de irregularidades graves, AGUILERA IZQUIERDO, R., "El derecho…", cit., p. 124; LAHERA FORTEZA, J., "Videovigilancia…", cit., pp. 274-275, si bien se decanta por limitarlo a la comisión de actos delictivos.

Respecto a los dispositivos digitales, en similar sentido de admisión excepcional a la luz de la jurisprudencia vigente, *vid.* GARCÍA RUBIO, M.A., "El control…", cit., pp. 170-172, con algún matiz cuando entra en juego el derecho al secreto de las comunicaciones; también, GOÑI SEIN, J.L., "Uso…", cit., p. 22; o *vid.* asimismo, NAVARRO NIETO, F., "Facultades…", cit., p. 252.

FERNÁNDEZ FERNÁNDEZ, R., "La geolocalización como mecanismo de control laboral: alcance y límites de una controvertida herramienta del poder directivo", *Revista de Trabajo y Seguridad Social. CEF* nº 452, 2020.

GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I.A., "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo* nº 216, 2019, BIB 2019\1432.

GARCÍA RUBIO, M.A., "El control sobre el uso de los ordenadores puestos a disposición de los trabajadores", en TALÉNS VISCONTI, E.E. y VALLS GENOVARD, M.A. (Dir.), *La actividad de los detectives privados en el ámbito laboral. Aspectos sustantivos y procesales de la obtención de la prueba*, Bosch Wolters Kluwer, Madrid, 2020.

GOÑI SEIN, J.L., "Uso de los dispositivos digitales en el ámbito laboral", *Trabajo y Derecho* nº 11/2020.

LAHERA FORTEZA, J., "Videovigilancia laboral y grabación de sonidos en el lugar de trabajo", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021.

LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., "Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral", en MONREAL BRINGSVAERD, E., THIBAULT ARANDA, X., JURADO SEGOVIA, A., *Derecho del trabajo y nuevas tecnologías*, Tirant lo blanch, Valencia, 2020.

MERCADER UGUINA, J.R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Francis Lefebvre, Madrid, 2019, 3ª ed.

MERCADER UGUINA, J.R., "Nuevas señales y paradojas de la protección de datos en la reciente doctrina de los Tribunales y de la Agencia Española de Protección de Datos", *Trabajo y Derecho* nº 85/2022.

MOLINA NAVARRETE, C., "Régimen legal de los sistemas de control laboral basados en la videovigilancia: lagunas y antinomias a la luz del Derecho Comunitario", en RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A. (Dir.), *Vigilancia y control en el Derecho del Trabajo Digital*, Aranzadi, 2020.

MOLINA NAVARRETE, C., "Eficacia de gestión versus protección de datos: ¿reactividad jurisdiccional a la «inflación de derechos humanos» (en el trabajo)? Comentario a la Sentencia del Tribunal Constitucional 160/2021, de 4 de octubre", *Revista de Trabajo y Seguridad Social. CEF* nº 465, 2021.

NAVARRO NIETO, F., "Facultades empresariales y garantías del trabajador en relación con el uso de dispositivos digitales en el ámbito laboral", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021.

ORELLANA CANO, A.M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores*, Aranzadi, Navarra, 2019.

PÉREZ DE LOS COBOS ORIHUEL, F., "Poderes del empresario y derechos digitales del trabajador", *Trabajo y Derecho* nº 59/2019.

RODRÍGUEZ CARDO, I.A., "Utilización de sistemas de geolocalización en el ámbito laboral", *Revista del Ministerio de Trabajo y Economía Social* nº 148, 2021.

RODRÍGUEZ ESCANCIANO, S., "Participación de los representantes de los trabajadores en el tratamiento de datos personales: derechos de información y consulta",

Jurisdicción social. Revista de la Comisión de lo Social de Juezas y Jueces para la Democracia, nº 197, 2019.

SERRANO OLIVARES, R., "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.