Ars Iuris Salmanticensis
ESTUDIOS
Vol. 7, 129-171
Junio 2019
eISSN: 2340-5155

Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno (RGPD 2016 y LOPDP-GDD 2018)

Protection of data and guarantee of digital labor rights in the new European and internal normative framework

Jesús Baz Rodríguez
Profesor Titular de Derecho del Trabajo
Universidad de Salamanca
jesusbaz@usal.es

Fecha de recepción: 15 de abril de 2019
Fecha de aceptación definitiva: 30 de mayo de 2019

Resumen

La Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDP-GDD) ha venido a formular, en el marco de su Título X, una regulación embrionaria de las garantías digitales de los trabajadores, a partir del mandato del RGPD de adaptar la normativa general de

Abstract

The Spanish Data Protection Act (LO 3/2018) has recently formulated an embryonic regulation about digital rights for workers, implementing the mandatory previsions contained in the European GDPR in order to adapt that holistic legal frame of data protection to the particular context of labour relations.

© Ediciones Universidad de Salamanca - CC BY-NC-ND

protección de datos al entorno laboral. Pese a su regulación minimalista, se erige, no obstante, a la normativa de protección de datos en su conjunto en referencia ineludible de gran relevancia en punto al establecimiento de límites al ejercicio de los poderes empresariales de supervisión laboral. Partiendo de dicha premisa, se regulan algunos de los escenarios social y jurisprudencialmente típicos en los que dicho ejercicio conlleva tratamientos de datos personales de los trabajadores, otorgándose a estos derechos de privacidad en relación con el uso de dispositivos digitales, la videovigilancia y captación de sonidos y la geolocalización. Derechos cuyo alcance y efectividad ha de construirse no solo a partir de su lacónica formulación legal, sino desde un enfoque sistemático.

Palabras clave: Privacidad de los trabajadores; protección de datos personales; dispositivos digitales en el trabajo; videovigilancia; grabación de sonidos; geolocalización; desconexión digital.

Even though its limitations, the new regulation points out to the whole legal system on Data Protection as an inescapable reference in order to build a complex set of limitations that should be respected by employers in the exercise of their labour managing and monitoring powers; particularly related to situations like the workers' use of digital devices at the workplace, videosurveillance, sound recording or locational surveillance.

Key words: *Privacy of workers; protection of data; digital devices at work; vidiovigilance; soun recording; geolocator; digital disconnect.*

1. LA NORMATIVA DE PROTECCIÓN DE DATOS COMO REFERENCIA PARA DELIMITAR LA OBLIGACIÓN POSITIVA DEL ESTADO EN LA PROTECCIÓN DE LA PRIVACIDAD DEL TRABAJADOR

La entrada en vigor del Reglamento General de Protección de Datos de la UE (en adelante, RGPD)[1], el cual supone no solo una actualización, sino un cambio de paradigma del modelo europeo de protección de datos, ha traído consigo la necesidad de adaptar la normativa interna en la materia: no solo para efectuar una labor de depuración del ordenamiento interno, reforzando la seguridad jurídica[2]; sino también para desarrollar la norma comunitaria en aspectos en los que esta lo precisa o prevé

1 Reglamento (UE) 2016/679, del Parlamento Europeo y el Consejo, de 27-4-2016 (*DOUE* 4-5-2016); en vigor desde el 25 de mayo de 2018.

2 *Vid.* Considerando 8 RGPD, que autoriza a integrar en normas nacionales las disposiciones de un Reglamento en aras de la claridad. Una previsión infrecuente y heterodoxa en un Reglamento de la UE, cuya aplicabilidad directa no requiere acto alguno de incorporación a los derechos internos. Téngase en cuenta, por otro lado, que el RGPD (Considerando 10) contempla la pervivencia de toda la normativa sobre protección de datos previa en los ordenamientos internos.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

expresamente. Así sucede precisamente con el tratamiento de datos personales en el ámbito laboral, donde el RGPD (artículo 88 y Considerando 155) renuncia expresamente a acometer una regulación uniforme en la materia, remitiéndose a las «normas más específicas» previstas en los derechos nacionales. Ahora bien, debe resaltarse el hecho de que, a diferencia de sus precedentes normativos, que ignoraban o desatendían por completo la relevancia del derecho a la protección de datos en su proyección sobre el ámbito del trabajo, el RGPD parte, en cambio, de afirmar con absoluta nitidez su plena vigencia en dicho contexto. Se estima necesaria, eso sí, la aprobación interna de disposiciones legales –y también convencionales– que adapten, complementen, refuercen o enriquezcan las reglas y principios contenidos en dicho cuerpo normativo «ómnibus», desde una óptica reguladora netamente protectora y tutelar[3].

Así las cosas, de entrada, el advenimiento del nuevo modelo normativo de protección de datos debe valorarse como un auténtico punto de inflexión, en cuanto que marca el cierre definitivo de la etapa de la resistencia frente la permeabilidad de la normativa de protección de datos en el ámbito de las relaciones laborales[4]. Tanto más a partir de la coincidencia –temporal y axiológica– entre la aparición del nuevo marco

3 En cuanto al contenido material de la normativa interna, el artículo 88 RGPD, no obstante, más que apuntar a resultados normativos definidos –al estilo, por ejemplo, de la armonización perseguida por una Directiva– se limita a aludir, de manera un tanto desordenada, a las siguientes cuestiones: 1) el objetivo general de la regulación (artículo 88.1), de carácter netamente tuitivo del contratante débil sometido a un vínculo de subordinación, consistente en «garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral». 2) Las materias, instituciones o áreas típicas del ordenamiento jurídico-laboral que se encuentran afectadas: contratación de personal; ejecución del contrato laboral; 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; disfrute individual o colectivo de derechos o prestaciones relacionados con el empleo; extinción del contrato de trabajo. 3) Los bienes jurídicos que están llamados a ser protegidos (artículo 88.2): preservación de la dignidad humana, de los intereses legítimos y de los derechos fundamentales de los trabajadores. 4) El eje central sobre el que debe girar la operación normativa: la transparencia del tratamiento, como valor instrumental –que informa transversalmente el RGPD en su conjunto– para conseguir la tutela. Y 5) Las dinámicas de actuación empresarial que agravan los riesgos para la privacidad de los trabajadores en la era de la globalización y *Big Data*: las transferencias de datos en las estructuras empresariales complejas (grupos de empresas y uniones de empresas dedicadas a una actividad económica conjunta) y los sistemas de supervisión laboral.

4 Una resistencia que se justificaba, para determinados sectores, en la inadecuación de la normativa «ómnibus» sobre protección de datos para su proyección sobre las relaciones laborales. *Vid.*, por ejemplo, GOERLICH PESET, J. M. 2016: «Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas». En AA. VV.: *El derecho a la privacidad en un nuevo entorno tecnológico*. Madrid: Centro de Estudios Políticos y Constitucionales, crítico con la opción de confiar «en una normativa, como es la de protección de datos, pensada para otras cuestiones (que) conduce a la aparición de un marco de elevada incertidumbre» (p. 148).

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

normativo y la decisiva reivindicación o reafirmación de la vigencia de los principios y la normativa sobre protección de datos efectuada por el TEDH a partir de su sentencia STEDH 5-9-2017 (Barbulescu II), cuya aportación esencial es la reformulación de los límites a los poderes empresariales utilizando justamente, como criterio fundamental de referencia, los principios y la normativa de protección de datos personales[5].

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de los Datos Personales y Garantía de los Derechos Digitales[6] (en adelante LOPDP-GDD), tal y como reza su propia denominación, responde a un doble propósito: la labor de adaptación de la legislación interna sobre protección de datos al RGPD se ha visto complementada por la intención de abordar, de modo pionero, la delimitación de un primer y embrionario marco normativo orientado a posibilitar el ejercicio de los derechos fundamentales de los ciudadanos en la realidad digital, en la estela de lo sucedido en otros ordenamientos. El Título X del texto legal («Garantía de los Derechos Digitales») aborda, de este modo, el reconocimiento de un sistema de garantía de los derechos digitales que, en expresión del Preámbulo de la norma, encuentra su anclaje precisamente en el mandato impuesto al legislador por el artículo 18.4 CE: la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Un marco normativo autoproclamado como provisional, en la medida en que propugna la necesidad de una reforma de la norma fundamental para su actualización a la era digital y, específicamente, para la futura elevación a rango constitucional de una nueva generación de derechos digitales[7].

Pues bien, es justamente en el contexto del Título X LOPDP-GDD donde el legislador español ha situado la normativa interna destinada a garantizar la protección de los derechos y libertades en relación con el tratamiento de datos de los trabajadores en el ámbito laboral, dando contenido material al reenvío formulado por el artículo 88 y el Considerando 155 del RGPD. Así se pone de manifiesto en el nuevo artículo 20 bis ET[8],

5 *Vid.* ampliamente GOÑI SEIN, J. L. 2018: «La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional». *Trabajo y Derecho*, 2018, 40: 12-26; estudio que consideramos una referencia doctrinal imprescindible para comprender plenamente el significado y las implicaciones de la jurisprudencia «Barbulescu II».

6 *BOE* 6-12-2018.

7 El inicial Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (*BOCG* 24-11-2017, Serie A, n.º 13-1) no contemplaba, empero, dicho doble objetivo legal. El enriquecimiento de los objetivos de la regulación, con el correspondiente añadido del Título X al texto («Garantía de los Derechos Digitales») que se desea resaltar en la propia denominación final del texto legal, se lleva a cabo a partir de la aprobación del Informe de la Ponencia elevado a la Comisión de Justicia del Congreso de los Diputados, como consecuencia de la aceptación de enmiendas y de las transacciones alcanzadas durante el debate en el seno de este (*BOCG* 9-10-2018, Serie A, n.º 13-3).

8 Introducido por la D.F. 13.ª LOPDP-GDD.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

que se encarga de efectuar una sucinta enumeración declarativa de derechos digitales laborales, cuyos términos de ejercicio quedan remitidos precisamente a lo regulado en la LOPDP-GDD:

> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Como punto de partida, la LOPDP-GDD ha decidido, así las cosas, dar cobertura legal únicamente a un primer núcleo iniciático de derechos digitales ejercitables en el ámbito laboral que se derivan del artículo 18.4 CE, con la vista puesta exclusivamente en determinados escenarios o situaciones típicas (tanto en el plano social como jurisdiccional), en las que se ha venido manifestando de manera más evidente la conflictividad –y la disparidad de criterios de ponderación– en torno a la protección de la privacidad de los trabajadores a lo largo de las últimas décadas: el acceso empresarial a mensajes electrónicos y otros archivos informáticos de naturaleza privada existentes en los ordenadores propiedad de la empresa, el control audiovisual, los sistemas de seguimiento, etc. Situaciones en las que existe, así pues, tal y como reconoce el Preámbulo de la norma (Apartado IV), una previa labor de perfilado técnico por parte de «la jurisprudencia ordinaria, constitucional *y europea*»; con resalte explícito, pues, de la doctrina del TEDH, que se declara así como una indudable referencia. El sistema legal de garantía se basa, en suma, en la escueta formulación de cuatro derechos digitales laborales:

a) El derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral (artículo 87 LOPDP-GDD);
b) El derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (artículo 89 LOPDP-GDD); y
c) El derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (artículo 90 LOPDP-GDD).
d) Menor conexión con el artículo 18.4 CE tiene, en cambio, el derecho a la desconexión digital en el ámbito laboral (artículo 88 LOPDP-GDD): un derecho orientado predominantemente a garantizar la efectividad de los tiempos de descanso, permiso, vacaciones, etc., que, si bien puede estar conectado con la protección de la intimidad personal y familiar, no lo está tanto, en cambio, con la protección de datos personales.

Es, de hecho, la influencia del artículo 8 CEDH, y de la construcción del TEDH en torno al mismo, la que explica, a nuestro juicio, la decisión del legislador interno de calificar estas garantías de los derechos digitales como atributos que cuelgan del derecho a la intimidad. Y es que, lo que a primera vista podría parecer una contradicción

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

con lo dispuesto en el Preámbulo de la norma (garantía de los derechos digitales como desarrollo del derecho autónomo previsto en el artículo 18.4 CE) no es realmente tal, por cuanto que los términos de ejercicio de tales derechos se regulan «en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales». Una remisión, la del artículo 20 Bis ET, que hay que entender efectuada, por cierto –lo cual resulta de trascendental importancia para comprender el impacto de la LOPDP-GDD– no solo a los concretos preceptos en los que se desarrollan los derechos aludidos en el nuevo precepto estatutario (artículos 87-91)[9], sino al conjunto normativo vigente globalmente considerado, encabezado hoy día por una normativa europea de aplicabilidad directa (RGPD, LOPDPD-GDD, normativa de desarrollo reglamentario no contraria a los mismos, etc.: en adelante NPD). El legislador español acoge así una técnica de remisión formal «en bloque» a la NPD inspirada quizá, en buena medida, en las coordenadas del Derecho alemán[10].

Es esta remisión en bloque a la NPD, de hecho, el efecto buscado y plenamente conseguido a través de la técnica de remisión formal, frente a la remisión material contenida en los textos preparativos de la norma (regulación dentro de la ley laboral del contenido del derecho): se apunta al conjunto de un complejo sistema de ordenación de la privacidad como referencia insoslayable para definir los límites al ejercicio de los poderes empresariales en el entorno digital. Si bien pueden resultar ciertamente cuestionables otros aspectos técnico-legislativos como el recurso a un precepto «Bis» –lo que podría dar quizá una cierta sensación de falta de coherencia reguladora o de improvisación–[11], en cambio, es la afirmación de la vigencia global de la NPD la que, lejos de restar autonomía a la normativa laboral, refuerza en este caso sus criterios de ordenación. Dicha remisión *in totum* es precisamente la que sirve también para generar

9 La técnica de la remisión formal ha sido cuestionada partiendo (restrictiva e infundadamente, a nuestro juicio) de entender el artículo 20 Bis ET como una mera remisión a los artículos 87 a 90 LOPDP-GDD. *Vid*., por ejemplo, EDITORIAL. 2019: «El derecho a la privacidad en el trabajo en la nueva Ley Orgánica de Protección de Datos: una mala regulación». *Ciudad del Trabajo*, 2019, 14, quien sitúa a la LOPDPD-GDD en la «tendencia intromisiva» de otras disciplinas en el Derecho del Trabajo, que restan autonomía a este, apreciable en algunas leyes recientes (*v. gr.*, Ley 39/2015 –supresora de la reclamación administrativa previa–; Ley 9/2017, sobre contratos del sector público, etc.) (p. 6).

10 En Alemania –quizá el país europeo más protector de la privacidad laboral–, el conjunto de las previsiones de la Ley Federal sobre Protección de Datos (*Bundesdatenschultzgesetz*, BDSG) resulta aplicable a la recopilación, al procesamiento y a la utilización de datos de los trabajadores en la empresa, con las particularidades aplicativas previstas en el artículo 32 BDSG y, adicionalmente, con la aplicación de las previsiones de la negociación colectiva. *Vid.* GRENTZBERGER, V. y KIRCHNER, J. 2018: «Data Protection and monitoring». En KIRCHNER *et al.: Key aspects of German Employment and Labour Law*. Frankfurt: Springer-Verlag GmbH, 135-151.

11 *Vid.* MOLINA NAVARRETE, C. 2018: «La Constitución social del trabajo ("decente"): ¿un divorcio entre el ideal normativo y la cruda realidad en busca del nuevo "convenio regulador" o de "reconciliación"?». *CEF-Trabajo y Seguridad Social*, 2018, 429: 24-25.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

un amplio ámbito de obligaciones positivas que se atribuyen al empleador como responsable del tratamiento de datos de sus empleados: aquellas contenidas en la normativa «ómnibus», de incuestionable aplicación al terreno de las relaciones laborales, y muy en particular a los escenarios legalmente contemplados por la LOPDP-GDD: en este caso, con las adaptaciones contempladas en artículos 87 y ss. y eventualmente por la negociación colectiva.

Sucede además que con este planteamiento el legislador español se sitúa en plena sintonía, nos parece, con el «valor añadido» esencial de la doctrina del TEDH: la observancia del conjunto de los principios en materia de protección de datos personales como coordenadas básicas dotadas de alcance general para la racionalización del ejercicio de los poderes empresariales derivados del contrato de trabajo en el entorno digital[12]. La LOPDP-GDD no solo recoge dicha premisa, sino que incluso la amplía, al remitirse no estrictamente a los principios de protección de datos (artículos 5 y ss. RGPD), sino a la NPD en su conjunto en la que estos se incardinan. De este modo, la opción técnica escogida por el legislador, aparentemente contradictoria o conceptualmente confusa (derechos de intimidad o de privacidad que se ejercen en los términos de la NPD), resulta a nuestro juicio dotada de justificación, en cuanto que persigue seguramente mantener viva la conexión de los derechos digitales laborales con la doctrina progresiva y evolutiva del TEDH enraizada en el artículo 8 CEDH (derecho a la protección de la vida privada y familiar)[13].

Téngase presente, en este sentido, que la construcción efectuada por parte del TEDH no hace sino racionalizar y formalizar los principios generales aplicables a la obligación positiva de los Estados de asegurar el respeto de la vida privada en el marco de las relaciones de trabajo, en relación con las funciones respectivas de la legislación y de la jurisdicción. Si bien el artículo 8 TEDH se orienta predominantemente a proteger

12 *Vid.*, de nuevo, GOÑI SEIN, J. L.: «La protección de las comunicaciones electrónicas del trabajador:…», *op. cit.*, 12, para quien la conclusión más importante que debe extraerse de la jurisprudencia «Barbulescu II» es que el legítimo ejercicio del control de las comunicaciones electrónicas del empleado encuentra su límite directo en el respeto de los principios de protección de datos, a los que se reconduce el ámbito de la válida actuación del empresario. Y, por tanto, es a la luz de los requisitos dispuestos por el RGPD como deben ser interpretados los límites. Principios que asumen, en todo caso, un alcance general, debiendo reconocerse a los mismos «un valor vinculante en relación a otros mecanismos de control tecnológico en la empresa» (p. 14).

13 Todo ello tiene como efecto, por cierto, el enriquecimiento del alcance regulador de los diversos preceptos laborales que hacen referencia a la intimidad. Desde la ampliación, a nuestro juicio, de los derechos laborales básicos del trabajador *ex* artículo 4.2 ET –bien que hubiese sido conveniente, como se ha apuntado, la modificación explícita de este precepto a través de la LOPDPD-GDD, como se hizo en su momento con la LOI (LO 3/2007)–. O también, por ejemplo, la proyección del aparato sancionador de la LISOS (artículo 8.11), donde se tipifican como infracción administrativa muy grave «los actos del empresario contrarios al respeto de la intimidad y consideración debida a la dignidad».

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

a las personas frente a las injerencias arbitrarias sobre su privacidad procedentes de los poderes públicos, pesan también sobre los Estados obligaciones positivas para hacer efectivos los derechos garantizados en dicho precepto entre particulares[14]. Se reconoce así a los Estados un margen relativamente amplio para apreciar la necesidad de regular las condiciones de protección de la privacidad en las relaciones laborales, pero sin que dicha latitud resulte ilimitada; teniendo en cuenta, por otra parte, que en defecto de regulación legal, correspondería, en último término, a los órganos jurisdiccionales asegurar –por lo que se refiere en particular a la adopción de medidas de supervisión laboral– que estas se efectúen con las garantías adecuadas y suficientes contra los abusos y las arbitrariedades.

Desde esta perspectiva, debe saludarse positivamente el hecho de que el legislador español haya decidido por fin recoger el guante lanzado por el TEDH asumiendo su papel regulador, de suerte que la observancia de la NPD (en su conjunto, se insiste) queda ahora garantizada a partir de una declaración del legislador interno –en sede, por cierto, del bloque de la constitucionalidad– como sistema normativo aportador de criterios vinculantes para la labor de ponderación que corresponde a los tribunales, concretándose y adaptándose el alcance de dicha normativa en un limitado, pero hasta ahora conflictivo, número de escenarios[15]. Téngase presente que el artículo 20.3 ET, calificado en alguna ocasión como un precepto «preinformático»[16], se situaba como tal lejos de cumplir con las exigencias marcadas por el TEDH en cuanto a la necesidad de contar con un soporte legal, entendido como un título de habilitación legal claro y suficiente, que ampare conductas de afectación de la privacidad, aportando un grado mínimo de calidad, concreción y previsibilidad[17]. La sumisión de los supuestos más

14 *Vid.* CASAS BAAMONDE, M. E. 2018: «Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral». *Derecho de las Relaciones Laborales*, 2018, 2: 111-112.

15 Manifestamos, pues, nuestra total disconformidad con lecturas de la LOPDP-GDD que señalan que la nueva regulación se formula «obviando en buena medida la doctrina Barbulescu-2»: *vid.* EDITORIAL: «El derecho a la privacidad…», *op. cit.*, 6. En sentido contrario, en cambio, ROJO TORRECILLA, E.: «Los derechos digitales en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Notas al Título X», para quien «cuando se leen tales preceptos en más de una ocasión parece que estemos leyendo las sentencias dictadas por el TEDH en el caso Barbulescu II o en el de López Ribalda» (El Blog de Eduardo Rojo: http://www.eduardorojotorrecilla.es/2018/12/los-derechos-digitales-laborales-en-la.html) (18/01/2019).

16 *Vid.* TASCÓN LÓPEZ, R. 2017: «Tecnovigilancia empresarial y derechos de los trabajadores (Intento de construcción de una regla conceptual en el Derecho del Trabajo español)». *Revista de Trabajo y Seguridad Social-CEF*, 2017, 415: 53.

17 Así lo denunciaba PRECIADO DOMENECH, C. H. 2017: *El derecho a la protección de datos en el contrato de trabajo*. Pamplona: Thomson Reuters Aranzadi, 252-253, para quien el artículo 20.3 ET no cumplía con los estándares europeos de previsibilidad mínimos de la ley

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

conocidos de tecnovigilancia a la NPD en su conjunto –incluyendo las reglas particulares– aporta ya un marco regulador completo y seguro de referencia para la ponderación de los intereses que entran en juego. Un marco cuya imposición viene de hecho a negar de manera frontal la premisa mayor del silogismo sobre el cual el artículo 20.3 ET venía formulado: la posible adopción por el empleador de «las medidas que estime más oportunas» de vigilancia y control de la actividad laboral, cuya dicción literal vulneraba sin duda, de manera frontal, las garantías derivadas del artículo 8 TEDH.

El imperativo, incluso urgente, de subsanar una situación normativa inaceptable a la vista de las exigencias de la jurisprudencia del TEDH –ya incluso proyectadas sobre el ordenamiento laboral español en la STEDH 9-1-2018 (Asunto López Ribalda)[18] explica– en alguna medida el enfoque limitado achacable a la Ley: esto es, el hecho de que el marco embrionario de garantías de los derechos digitales se centre exclusivamente en materias relacionadas con la supervisión en el entorno laboral; la cual constituye solo una de las materias laborales aludidas por el artículo 88 RGPD. La LOPDP-GDD se sitúa así muy lejos de agotar toda la miríada de escenarios y situaciones –algunos de ellos apuntados por los textos y documentos internacionales más relevantes en la materia– en las que el tratamiento de datos personales de los trabajadores en el ámbito de la empresa merece una atención específica, y cuentan con un bagaje de elaboración técnica reseñable al respecto.

El limitado y escueto elenco de garantías digitales previsto legalmente se cierra, en fin, con la remisión a la negociación colectiva del establecimiento de «garantías adicionales» de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral: artículo 91 LOPDPD-GDD («Derechos digitales en la negociación colectiva»). Se remite así a la esfera de la autonomía colectiva el cumplimiento de una doble tarea:

1) Por una parte, con un carácter más inmediato, la de concretar, complementar, adaptar y eventualmente mejorar la protección básica dispensada por el legislador a los trabajadores en los escenarios previstos por la norma (uso de dispositivos digitales, videovigilancia y grabación de sonidos y geolocalización): se confía así en el carácter

habilitante exigidos, por ejemplo, en las Sentencias *Kruslin c. Francia* de 24 de abril de 1990, *Huvig c. Francia* de 24 de abril de 1990 o *Copland c. UK*: no se trata solo de que las medidas restrictivas del derecho contenido en el artículo 8 CEDH tengan un fundamento en el derecho interno, sino que también se refieren a la calidad de la norma: debe ser accesible a la persona afectada, que ha de poder prever sus consecuencias, y compatible con la preeminencia del derecho.

18 Téngase presente que dicho pronunciamiento –pendiente aún de ratificación por la Gran Sala– vino precisamente a corroborar la incompatibilidad del ordenamiento laboral español con las exigencias del artículo 8 CEDH (en contraste con la legislación alemana –Asunto Köpke– en la que se hallaba claramente regulado y protegido por ley el derecho del sujeto de observación a ser informado de la existencia, objetivo y modo de la videovigilancia encubierta. *Vid.* Apartado 67).

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

adaptativo y transaccional de los convenios colectivos para desarrollar el esquema tutelar legalmente previsto, precisando los límites a los poderes empresariales en atención a las características de cada ámbito productivo. La expresión «garantías adicionales» recordaría implícitamente, en todo caso, que no es posible la disponibilidad colectiva de los derechos fundamentales individuales, de suerte que el convenio no viene llamado a intervenir sobre la vertiente individual del derecho fundamental, sino respecto de la racionalización de los poderes del empleador en orden a la dirección y control del proceso productivo[19].

2) Pero, además de lo anterior, la aspiración de la norma quizá sea también la de confiar a la negociación colectiva la contemplación progresiva –dispensando «garantías adicionales» a las de la ley–, de pautas de ordenación en relación con otros muchos escenarios, situaciones y áreas típicas del ordenamiento laboral, diferentes de las aludidas legalmente, en las que se produce una afectación a la privacidad de los trabajadores a través del tratamiento de sus datos personales, a la vista tanto del artículo 88 RGPD, como de los documentos internacionales elaborados en el marco del Consejo de Europa y de la UE[20]. La génesis del Título X como una normativa de origen transaccional entre posturas muy polarizadas en sede parlamentaria[21], unida a las especiales circunstancias políticas del momento de la aprobación de la norma, son hechos que han condicionado decisivamente quizá la autolimitación en que incurre el

19 *Vid.* BAYLOS GRAU, A. 2019: «Una nota sobre el papel de la negociación colectiva en la configuración de los derechos derivados de la Ley de Protección de Datos Personales y Garantía de Derechos Digitales». *Ciudad del Trabajo*, 2019, 14: 154-159.

20 La LOPDP-GDD, al situar en la órbita institucional de la protección de datos la construcción de los derechos digitales laborales, aporta ahora un indudable valor, a nuestro juicio –a los efectos tanto de interpretación como de desarrollo del marco normativo–, a determinados documentos europeos e internacionales que constituyen auténticas referencias en la materia, también, por cierto para el TEDH: 1) La Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre el tratamiento de datos de carácter personal en el ámbito del trabajo, adoptada el 1 de abril de 2015. 2) Los sucesivos Documentos de Trabajo y Opiniones formulados por el Grupo de Trabajo del artículo 29 de la UE (GT 29), especialmente, aunque no solo, los enfocados en la temática laboral: Opinión 8/2001, sobre el tratamiento de datos personales en el contexto del empleo, de 13 de septiembre de 2001 (WP 48); Documento de Trabajo sobre la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, de 29 de mayo de 2002 (WP 55); y finalmente, recogiendo y complementando los anteriores, ya tras la aprobación del RGPD, la Opinión 2/2017, sobre el tratamiento de datos en el trabajo, de 8 de junio de 2017 (WP 249). 3) Todo ello, sin olvidar el Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores elaborado por la OIT en 1997 (RRP-OIT 97); instrumento más alejado en el tiempo y carente de carácter obligatorio, pero que se declara utilizable «para elaborar leyes, reglamentos, convenios colectivos, directivas y políticas laborales y disposiciones de orden práctico en el nivel de la empresa».

21 *Vid.* MIÑARRO YANINI, M.: «Impacto del reglamento comunitario de protección de datos en las relaciones laborales: un –pretendido– "cambio cultural"». *cef-TRABAJO Y SEGURIDAD SOCIAL*, 423: 13-14.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

legislador. Y en todo caso, ante la vertiginosa evolución de las técnicas de gestión del trabajo, este no tiene, ciertamente, una capacidad de respuesta inmediata, aspirando únicamente a diseñar un núcleo germinal de derechos digitales laborales cuya existencia y diseño técnico puedan servir para inspirar la creación progresiva de otros, a partir de un método «multinivel» de aproximación y de diseño técnico.

2. EL DERECHO A LA PRIVACIDAD DE LOS TRABAJADORES Y EL USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL

El artículo 87 LOPDP-GDD contempla el escenario básico a partir del cual, en buena medida, se ha venido generando el caldo de cultivo del «derecho a la vida privada social» del trabajador en su puesto de trabajo proclamado por el TEDH: la utilización de dispositivos digitales en el ámbito laboral suministrados por el propio empleador para el desempeño de la actividad laboral[22]. La interceptación y la monitorización del uso de las comunicaciones electrónicas en el lugar de trabajo (telefonía, internet, correo electrónico, mensajería instantánea, voz sobre IP, etc.), no en vano, han venido situándose en el centro de la elaboración teórica sobre la privacidad en el ámbito laboral desde hace tiempo –muy en particular, en los documentos procedentes del GT 29–[23], así como también, como es sabido, la propia labor jurisprudencial en los distintos niveles. Con su formulación amplia y genérica, el precepto tiene bien presente, no obstante, que el desarrollo tecnológico actual exige abarcar la existencia de una fenomenología muchísimo más amplia, compleja y sofisticada, que acaba abriendo la vía a posibilidades de llevar a cabo prácticas de monitorización de los trabajadores mucho más invasivas y penetrantes que anteriormente.

A partir del recurso cada día más accesible a múltiples tipos de herramientas combinadas y de paquetes tecnológicos integrales destinados en principio a preservar la integridad y seguridad de sus equipos y redes, la empresa se sitúa, hoy día, en condiciones de efectuar un seguimiento total y absoluto del uso de las TIC por parte del trabajador[24].

22 No contempla el precepto, en principio, los supuestos en que se permite la utilización de dispositivos propiedad del empleado para uso laboral (BYOD: *Bring your own device*), que plantean una problemática singular al ampliarse enormemente las posibilidades de que el empleador trate información no corporativa sobre los empleados.

23 *Vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», de 29 de mayo de 2002 (WP 55), como texto de referencia aún hoy imprescindible en la materia, pese a estar centrada su atención en el uso de internet y el correo electrónico en los lugares de trabajo.

24 *Vid.* WP 29: «Opinion 2/2017 on data processing at work», *op. cit.*, 12-13: desde herramientas de prevención de la pérdida de información (DLP o *Data Loss Prevention*), que controlan

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

En la medida en que los trabajadores desarrollan una parte significativa de su relación social en o desde el puesto de trabajo, se afirma la existencia de una expectativa legítima de un cierto grado de privacidad del empleado, que ha de equilibrarse con los derechos e intereses del empleador, vinculados estos no solo con la búsqueda de la eficiencia empresarial, sino también incluso con la posible responsabilidad derivada de las actuaciones de sus empleados. No obstante, la mera conveniencia de llevar a cabo tales prácticas de interceptación y/o monitorización para servir a los propósitos empresariales no justifica por sí misma la intrusión en la privacidad: es preciso, *con anterioridad* a la implementación de las medidas correspondientes, su sometimiento a un examen de compatibilidad con los principios que rigen el tratamiento de datos, contemplados actualmente en el artículo 5 RGPD (licitud, lealtad, transparencia, minimización de datos, limitación de la finalidad, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva). Principios cuya observancia pasa por el establecimiento de políticas de empresa claras sobre el uso de los dispositivos digitales, partiendo siempre de asumir una premisa básica en este terreno: que la prevención de los usos desviados de los dispositivos digitales debe ser más importante que la detección de los mismos, en punto a lograr el máximo grado de consecución simultánea de los intereses confrontados.

Pues bien, a partir de estas coordenadas –largamente afirmadas por el GT 29 y actualmente reforzadas por el TEDH–, el artículo 87 LOPDP-GDD aborda una serie de aspectos que se analizan seguidamente:

1) *La proclamación formal de un derecho modulable, pero no eliminable de manera discrecional en la empresa*: La primera aportación del precepto es la proclamación formal, dentro del bloque de constitucionalidad, de un derecho cuya existencia resultaba controvertida, al menos hasta la STEDH 5-9-2017 (Barbulescu II), en sede de la jurisprudencia interna (constitucional y ordinaria): los trabajadores «tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador». Su propia enunciación como una derivación del artículo 18 CE

y almacenan todas las comunicaciones electrónicas para detectar posibles pérdidas de información, hasta sistemas y aplicaciones que combinan una variedad de tecnologías de monitorización y filtrado de contenidos, conexiones y datos de usuarios (*Next Generation Firewalls, Unified Threat Management*, etc.); pasando por aplicaciones de seguridad que implican el registro de accesos a los sistemas informáticos del empleador; procesos de almacenamiento de datos electrónicos para ser utilizados como prueba de anomalías *(EDiscovery technology)*; programas ocultos de registro detallado del uso de aplicaciones o equipos que se encuentran instalados sin conocimiento del usuario en el mismo, o que operan desde la nube; aplicaciones «office» disponibles como servicios en la nube que permiten un registro detallado de las actividades digitales del empleado; etc. Todo ello hasta llegar a la posibilidad de que el empleador ponga en práctica soluciones integrales de monitorización *(«all-in-one» monitoring solutions)* que le capacitan para efectuar un auténtico control integral o total del uso de las TIC efectuado por el trabajador.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

podrá permitir que queden modulados o afectados los términos de su ejercicio, o bien limitado su alcance cuando –y en la medida en que– ello resulte imprescindible para la atención a intereses legítimos del empleador, adoptándose las debidas garantías para el trabajador. Pero lo que ya no resulta admisible es la eliminación absoluta e injustificada de este derecho a la intimidad en el uso de los dispositivos digitales a partir del libre albedrío empresarial en la adopción de sus decisiones técnicas y organizativas. Así las cosas, la implementación, por ejemplo, de medidas de monitorización basadas en la necesidad de proteger los equipos informáticos y los datos manejados por la empresa no pueden conducir a efectuar un control integral de la actividad en línea del trabajador, sin que se haya analizado y descartado antes la posibilidad de recurrir tanto a medidas de prevención como a otros medios menos invasivos para la satisfacción de dicho interés legítimo (*v. gr.*, configuración de las aplicaciones que evite un registro permanente de la actividad del trabajador mediante el bloqueo del tráfico sospechoso entrante o saliente, o que minimice la información registrada, o que condicione esta a la detección de incidentes técnicos, etc.).

En este sentido, la norma viene a alinearse con una construcción de la jurisprudencia del TEDH a la que viene a aportar marchamo de ley: el establecimiento de prohibiciones para usos personales, aún totales, de los medios informáticos de la empresa puestos a disposición de los trabajadores no puede privar de relevancia a las expectativas de intimidad y al secreto de las comunicaciones del trabajador ni, en definitiva, eliminar completamente la expectativa razonable de privacidad[25]. Ello impone, sin duda, la necesidad de superar determinadas pautas anteriormente asumidas por la jurisprudencia constitucional interna[26], puesto que el reconocimiento de un derecho, por definición, viene de modo palmario a sancionar legalmente el principio de que el empresario no goza de una libertad total e incondicionada a la hora de configurar las posibilidades de controlar la utilización de los instrumentos digitales puestos a disposición del trabajador, desatendiendo un núcleo indisponible de tutela de su privacidad. El empresario no puede ya, por ejemplo, acceder al contenido de mensajes electrónicos del trabajador, por el mero hecho de haber prohibido el uso no profesional de los medios informáticos (como autorizaba la STC 241/2012), sino que tendrá que valorarse de manera casuística la concurrencia de determinadas condiciones de validez de tal

25 En la formulación literal del TEDH, «las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, aunque pueda limitarse dentro de las medidas de necesidad» (STEDH 5-9-2017, Barbulescu II, parágrafo 80).

26 *Vid.*, una vez más, GOÑI SEIN, J. L.: «La protección de las comunicaciones electrónicas del trabajador:…», *op. cit.*, 22-26; CASAS BAAMONDE, M. E.: «Informar antes de vigilar…», *op. cit*., 116-119. Autores que señalan concretamente a la definitiva superación de la doctrina constitucional fijada en las conocidas SSTC 241/2012 y 170/2013, basadas en asunciones ya inadmisibles a partir de Barbulescu II.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

comportamiento. Del mismo modo que tampoco una disposición general incluida en un convenio colectivo sancionando la utilización para fines particulares de los medios informáticos por parte del trabajador (STC 170/2013) es suficiente para considerar que se puedan controlar los correos electrónicos del trabajador sin necesidad de transparencia e información previa, y sin que el propio convenio colectivo contemple garantías adecuadas y suficientes frente al abuso en el control[27].

2) *El acceso empresarial a los contenidos derivados del uso de los medios digitales por los trabajadores: la acotación de las bases jurídicas de licitud*: En este aspecto reside, a nuestro juicio, la aportación más relevante del artículo 87, al determinar que, con carácter general, dicho acceso tendrá lugar «a los solos efectos de controlar el cumplimiento de las obligaciones laborales» y de «garantizar la integridad de dichos dispositivos» (artículo 87.2). De este modo, el precepto viene nítidamente a acotar las dos únicas bases de licitud que puede esgrimir el empleador para acceder a los contenidos de los dispositivos digitales, al tiempo que también a concretar o especificar su alcance en cada caso, en atención a los principios de necesidad y de limitación de la finalidad: a) El carácter necesario de la medida para la ejecución del contrato (artículo 6.1 b) RGPD), que ha de interpretarse, de modo estricto, como relativo al control del cumplimiento de las obligaciones de naturaleza laboral. O bien, b) La satisfacción de un «interés legítimo» del empleador (artículo 6.1 f) RGPD), que se reduce exclusivamente a la garantía de la integridad (o seguridad) de los dispositivos digitales; esto es, a la necesidad de proteger la propia red informática empresarial y también todo el conjunto de datos personales de clientes, trabajadores, etc., quedando cerrada en principio, a nuestro juicio, la apelación a dicho título legitimador genérico para cualquier otro propósito empresarial.

Queda excluida por la norma, desde luego, la apelación al consentimiento del trabajador (artículo 6.1 a) RGPD) como vía alternativa, en cualquier forma, para habilitar el acceso empresarial a dichos contenidos sin acogerse a alguno de los dos supuestos anteriores. Resultan ilícitas, así pues, no solo las estipulaciones o pactos que de modo abierto e injustificado contemplen, por ejemplo, la aceptación por parte del trabajador de la instalación de determinadas aplicaciones que habiliten para el control integral de su actividad en los dispositivos digitales[28], sino también cualesquiera de las

27 Exigencia para el convenio colectivo subrayada especialmente por el artículo 9.2 b) RGPD con motivo del tratamiento de categorías sensibles de datos personales, pero que se derivaría, con carácter general, de la proyección del «test Barbulescu» de legitimidad.

28 *Vid.* un amplio repertorio ejemplificativo en SOLON, O. 2017: «Big brother isn't just watching: workplace surveillance can track your everymove» (www.theguardian.com, 6 noviembre 2017) (1/12/2017). Los proveedores de «tecnologías de vigilancia», partiendo de su experiencia en la publicidad y el sector financiero –en el que las empresas han estado legalmente obligadas a rastrear las comunicaciones entre sus subordinados para prevenir el uso en provecho propio

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

múltiples vías que en la práctica pueden acabarse utilizando, de modo más o menos subrepticio, para dar cobertura a la práctica ilegal de la habilitación «consentida» de la supervisión[29].

Se trata, además, de dos títulos jurídicos de actuación supervisora que han de entenderse como autónomos y diferenciables. Lo cual acarrea una importante consecuencia: no resulta lícito, en definitiva, por resultar incompatible con el principio de limitación de la finalidad, que las medidas adoptadas con miras a garantizar el funcionamiento seguro de los sistemas informáticos se utilicen para vigilar y juzgar el comportamiento o el rendimiento de los trabajadores. Es esta, de hecho, una premisa nítidamente proclamada por el GT 29[30], ya reflejada en alguna ocasión a nivel interno[31]. Por otra parte, el acceso por el empleador al contenido de dispositivos digitales

---

de información provilegiada (*inside trading*)–, parecen haber ido extendiendo su nicho de mercado a otros sectores interesados en la filtración de datos sensibles, en la monitorización del comportamiento y la productividad o la represión de actuaciones inadecuadas por parte de los empleados. Se describen así, en este interesante trabajo divulgativo, una amplia variedad de productos y herramientas informáticas diseñados «ad hoc» por consultoras especializadas, así como una serie de aplicaciones, tales como *WorkSmart*, *Facebook Workplace*, *Slack*, *Yammer*, *Fama* y similares, concebidas tanto para monitorizar –y estimular– la productividad, como para actuar frente a comportamientos desviados de los empleados, tomando como base desde la detección de términos y expresiones tecleadas, la frecuencia en el cambio entre las aplicaciones utilizadas, el número de mensajes, su extensión, la actuación en redes sociales, etc. El resultado es, casi siempre, la puesta en conexión de aspectos de la vida personal y la vida profesional; y la propia formulación de «asunciones» o prejuicios sesgados, no siempre justificados o admisibles, entre características personales y comportamientos relevantes en el ámbito profesional (*v. gr.*, propensión de trabajadores divorciados a cometer fraudes para satisfacer sus necesidades económicas; presuntas referencias no siempre acreditables a alcohol y/o drogas; pertenencia a entornos sociales o raciales determinados, etc.). Todo ello amparado, en determinados contextos jurídicos nacionales (*v. gr.*, EE. UU.), por la introducción de cláusulas en los contratos de trabajo que ampararían de manera global *(catch-all clauses)* el recurso a tales instrumentos de monitorización u otros similares.

29 *V. gr.*, firma de aceptación de protocolos de supervisión, firma acreditativa de la recepción de documentos informativos, cuya literalidad transite de la mera función probatoria del cumplimiento de la función informativa (principio de responsabilidad proactiva) a la aceptación expresa o tácita por parte del trabajador de los protocolos de supervisión, etc. Cosa distinta es, desde luego, la utilización de anexos al contrato de trabajo como vía de información al trabajador sobre las reglas de uso de los dispositivos digitales y los protocolos de supervisión, siendo la firma del anexo un posible medio para acreditar el cumplimiento de sus obligaciones informativas, tal y como ha reconocido la AEPD (Informe 0464/2013). *Vid.* MERCADER UGUINA, J.: *Protección de datos en las relaciones laborales*, *op. cit*., 115.

30 *Vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», de 29 de mayo de 2002 (WP 55). Anteriormente también, *cfr.*, a título de recomendación, los principios generales formulados por la OIT (principio 5.4) (R-OIT 97: 2 y 14).

31 La conocida STS 26-9-2007 (RCUD 966/2006) acababa declarando la improcedencia del despido por haber aprovechado el empresario los datos obtenidos de un registro del equipo

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

respecto de los que haya admitido su uso con fines privados, *ex* artículo 87.3, puede quedar restringida a límites adicionales de carácter temporal, habiendo el empresario de respetar la privacidad laboral de los trabajadores en los momentos en que se haya autorizado un uso privado, limitándose en la práctica el acceso a los dispositivos electrónicos por razones de control del cumplimiento de las obligaciones laborales en tales fases temporales, en las que el acceso deberá fundamentarse más bien, de manera predominante o quizá incluso exclusiva, en el segundo título de legitimación; esto es, en la concurrencia de un interés legítimo en punto a proteger la integridad de los sistemas informáticos[32].

Centrándonos en el acceso al contenido de los dispositivos digitales con fines de control laboral, hay que decir que su licitud ha de pasar con carácter general –según la construcción consolidada del GT 29– por descartar previamente otros métodos de supervisión tradicionales para el logro de la concreta finalidad perseguida. La observancia del principio de necesidad impone, desde luego, la exigencia de una valoración cautelosa, efectuada con carácter previo, que evidencie el carácter imprescindible de dicho acceso, no sustituible por otros cauces no tecnológicos que satisfagan con igual eficacia la facultad empresarial de supervisión. En este sentido, se ha venido afirmando precisamente el *carácter excepcional* del acceso empresarial a los dispositivos digitales utilizados por el trabajador –inicialmente en relación con el uso del correo electrónico y de internet–, cuya licitud ha de venir condicionada predominante, aunque no exclusivamente, a la necesidad de obtener confirmación o prueba de actuaciones del trabajador que impliquen la comisión de conductas irregulares o delictivas, así como de cualesquiera otras que pudiesen desencadenar la responsabilidad del empleador por los actos de sus empleados[33]. Sobre este punto ha de proyectarse especialmente, desde luego, la exigencia de transparencia, de modo que los trabajadores cuenten previamente con la suficiente información sobre qué circunstancias justifican la adopción de medidas de carácter tan excepcional, así como el alcance y profundidad de las actuaciones de monitorización que se puedan realizar.

---

informático cuya finalidad era reparar los fallos detectados en el ordenador, para otra finalidad diferente e incompatible, como es la adopción de medidas disciplinarias.

32 En este sentido, *vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», 15.

33 *Vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», 13-14. De este modo, ante la detección de conductas de uso desviado de los dispositivos electrónicos, a menos que existan razones que aconsejen la continuación de la vigilancia, una buena práctica podría consistir, por ejemplo, en el recurso a sistemas técnicos de información en forma de alertas (*promp information systems*, *warning windows*, *pop ups*, etc.) que disuadan al trabajador de continuar con dichas prácticas, evitando preventivamente la necesidad de un posterior acceso empresarial.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

Pues bien, asumiendo este planteamiento, la ley viene a otorgar base de legitimación, en principio, a los denominados «controles defensivos»[34], esto es, a los dirigidos a comprobar las conductas ilícitas cometidas por los trabajadores. La existencia de indicios fundados (no de meras sospechas) de comisión de actos ilícitos de carácter grave constituye, en este sentido, el presupuesto de partida fundamental que aporta un motivo legítimo a la actuación de supervisión. Se trata de un presupuesto de licitud ineludible para este tipo de controles defensivos: no sería tal, por ejemplo, el acceso a los dispositivos electrónicos facilitados por la empresa, con la finalidad simplemente de comprobar si el empleado hace o no un uso correcto de los mismos[35]. Junto a los controles defensivos, el artículo 87 LOPDP-GDD también puede aportar base de legitimación, a nuestro juicio, para llevar a cabo «controles indirectos» de la actividad laboral, entendiendo por tales a las actuaciones de supervisión para la consecución de finalidades organizativas o productivas legítimas, si bien dando lugar con ello, de manera derivada, a un conocimiento de la actividad del trabajador[36]. El WP 29 ha venido admitiendo, por ejemplo, la licitud del acceso a la correspondencia electrónica profesional del trabajador en los casos de ausencia de este (enfermedad, vacaciones, permisos, etc.), cuando ello resulta necesario para el mantenimiento de dicha correspondencia, al no poderse garantizar la misma de otro modo (*v. gr.*, mediante la activación de funciones de respuesta automática o de desvío automático de los mensajes)[37]. La realización de tareas o cometidos necesarios para el normal desarrollo de la actividad empresarial, especialmente en los supuestos de ausencia del trabajador (*v. gr.*, consulta de documentos, acceso a condiciones contractuales pactadas con un cliente, etc.), puede aportar un motivo legítimo para el acceso a los contenidos de los dispositivos digitales. Pero a diferencia de los controles defensivos, la información obtenida a través de los controles indirectos no permite, con carácter general, su utilización a efectos disciplinarios, salvo que exista la debida conexión entre el objeto de

34 Siguiendo la denominación de GOÑI SEIN, J. L.: «La protección de las comunicaciones electrónicas…», *op. cit.*, 20.

35 Así parece deducirse del razonamiento seguido por el TEDH en la Sentencia Barbulescu II, parágrafo 135, al cuestionarse por la justificación de la medida enjuiciada (acesso al contenido de mensajes electrónicos), no existiendo una acusación concreta de actividad ilegal.

36 Sobre el concepto de «vigilancia indirecta», *vid.* inicialmente la Recomendación OIT-97, pp. 20-21, referido a sistemas instalados con fines diferentes del control de la actividad laboral (observación y análisis de operaciones, dispositivos de contabilización de las llamadas telefónicas y de información sobre el personal, etc.), pero que permiten recabar datos que pueden transformarse con facilidad en medios de vigilancia.

37 *Vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», p. 14.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

control y la anomalía detectada: no se respetaría, en tal caso, el principio de limitación de la finalidad (artículo 5.1 b) RGPD)[38].

3) *La cuestionable licitud de los usos secundarios de la información*: La severidad de la formulación legal del artículo 87.2 LOPDP-GDD –acceso «a los solos efectos» de controlar el cumplimiento de las obligaciones laborales– plantea, a nuestro juicio, una importante cuestión. Junto a la trascendente acotación de las bases de legitimidad para la monitorización, la intención del legislador quizá haya sido también la de reforzar el principio de limitación de la finalidad, hasta llegar a formular una auténtica prohibición de realizar usos secundarios de los datos e informaciones obtenidos a partir del acceso a los dispositivos digitales utilizados por los trabajadores. El precepto podría contener también, así las cosas, una excepción o «blindaje» con respecto de la aplicación de la previsión genérica del RGPD que prevé la licitud excepcional de los «usos secundarios» de los datos obtenidos para una finalidad distinta, pero compatible, en el sentido del artículo 6.4 RGPD. Lo cual convertiría en intransitable la posibilidad de reutilizar la información obtenida a partir de la monitorización de los dispositivos digitales de los trabajadores con fines de control laboral, en atención a la ponderación de las circunstancias allí señaladas (relación entre los fines primarios de obtención de la información y los usos secundarios, contexto y relación entre los interesados –*v. gr.*, expectativas de utilización futura de la información–, naturaleza de los datos, posibles consecuencias del tratamiento ulterior, existencia de garantías adecuadas, etc.). El marco legal autoriza la recogida de datos derivados del uso de los dispositivos digitales *(data collection)* acogiéndose a bases de licitud para el acceso bien delimitadas; pero quizá obtura su ulterior procesamiento *(data processing)* para otras finalidades diversas, sean o no consideradas compatibles.

Existe, a nuestro juicio, una sólida base argumental para sostener que el artículo 87 LOPDP-GDD prohíbe la reutilización de la información extraída a partir del acceso a los dispositivos digitales utilizados por los trabajadores para finalidades diferentes de las que justificaron la concreta medida de control empresarial, sin que resulte admisible quizá ninguna operación que pondere su hipotética consideración como «compatibles». Debe tenerse bien presente, como punto de partida, el carácter excepcional, reforzado normativamente, que reviste el acceso empresarial a los dispositivos digitales utilizados por el trabajador, cuya licitud queda exclusivamente condicionada a la concurrencia de propósitos concretos –que deben ser previa y convenientemente delimitados–, de control laboral[39]. Es justamente este entendimiento en clave excepcional,

38 *Vid.* GOÑI SEIN, J. L.: «La protección de las comunicaciones electrónicas…», *op. cit.*, pp. 20-21.

39 Un carácter excepcional –formulado inicialmente por el GT 29 en atención básicamente al correo electrónico e internet– que se debe seguir afirmando como criterio consolidado en la construcción técnica sobre el derecho a la vida privada social del trabajador. Así lo confirma, de

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

junto a la propia literalidad del precepto, el que añade un peso argumental decisivo a la interdicción de los usos secundarios de la información obtenida: atendiendo a dicho criterio, parece razonable pensar que la opción del texto legal ha sido la de prohibir *iuris et de iure* la reutilización de información obtenida con fines de control laboral, para su empleo posterior en atención a otras finalidades o propósitos decisorios o de ordenación técnico-laboral diferentes. El precepto vendría quizá a negar la compatibilidad del fin, sin llegarse siquiera a permitir la operación de ponderación *(iuris tantum)* a la que remite el artículo 6.4 RGPD a tal efecto.

Se trata de una interpretación que guarda sintonía, por lo demás, con el carácter tutelar y protector que atribuye el artículo 88 RGPD a la ley interna de adaptación del marco general sobre protección de datos al contexto laboral. Enfocado el RGPD en la vertiente de otorgar protección en la fase de recopilación de datos personales, en detrimento de las fases ulteriores de análisis y utilización de los mismos para finalidades decisionales –donde el alcance tutelar de las previsiones reglamentarias resulta más limitado–[40], la normativa interna laboral que lo complementa habría decidido formular reglas particulares, incrementando la intensidad protectora dispensada por marco general en este punto. De acogerse esta lectura de la norma, rigurosa con la exigencia del principio de limitación de la finalidad, la LOPDP-GDD habría venido a establecer serias limitaciones jurídicas a la puesta en práctica de técnicas analíticas (*workforce analytics, Big Data*, etc.) utilizadas para la toma de decisiones en materia de gestión del trabajo que precisen del empleo de datos y metadatos procedentes de los dispositivos electrónicos utilizados en el puesto de trabajo[41].

4) *El deber empresarial de establecer «criterios de utilización» de los dispositivos digitales en la empresa*: La proclamación del derecho del trabajador a la privacidad en el uso de los dispositivos digitales no equivale a eliminar la idea de la variabilidad del alcance del poder de vigilancia del empresario, en función de la configuración que

---

hecho, más recientemente el GT 29, remitiéndose a la validez global del planteamiento efectuado en 2002 (WP 29: «Working Document on the surveillance of electronic communications in the workplace»), al que se remite íntegramente en los tiempo más recientes: *vid.* WP: *Opinion 2/2017 on data processing at work*, *op. cit*., 12.

40 *Vid.* WATCHER, S. 2019: «Data protection in the age of Big Data». *Nature Electronics*, 2019, 2, January: 6-7.

41 Sobre la caracterización de *Big Data* en el contexto del empleo, *vid.* TRINDEL, K. 2016: «Written testimony», *Public Meeting on Big Data in the Workplace*. US Equal Employment Opportunity Commission, 13-10-2016. El cual se basa esencialmente en la combinación de datos «no-tradicionales» procedentes de todo tipo de fuentes de información digitalizada, con datos «tradicionales» sobre rendimiento, comportamiento y ejecución del contrato de trabajo, para así elaborar «perfiles» de los empleados y candidatos al empleo –a partir de la formulación de algoritmos y modelos estadísticos– utilizables ulteriormente para la adopción de todo tipo de decisiones empresariales afectantes a la esfera laboral.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

este efectúe de las condiciones de disposición y uso de las herramientas informáticas, y de las instrucciones que dicte el empresario a tal fin[42]. Antes bien, la norma toma la decisión de reforzar el principio de transparencia, asignando al empleador un deber de establecer «criterios de utilización» de los dispositivos digitales. Si bien subrayando, al mismo tiempo, que dicha tarea no puede ya abordarse de un modo completamente libre o incondicionado, sino «respetando en todo caso los estándares mínimos de protección de su intimidad, de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente» (artículo 87.3 LOPDP-GDD). La mera conveniencia de contar en las empresas con instrumentos formalizados, unilaterales o negociados, en los que quede formulada de un modo claro la política empresarial en cuanto al uso de los medios digitales (políticas de usos razonables) y las garantías de privacidad para los trabajadores en relación con los controles proclamada por los textos internacionales y la jurisprudencia interna –desde la conocida STS 26-9-2007–[43] es elevada ahora a deber legal. Tales reglas de uso, hay que entender, deben contar con un soporte mínimamente formalizado que propicie su general difusión, conocimiento y, en su caso, sucesivas actualizaciones. Es esta, de hecho, la opción normativa que resulta más coherente con las coordenadas del actual modelo de protección de datos (transparencia, principio de responsabilidad proactiva, incorporación de la protección de datos a la cultura y dinámica de la organización, etc.)[44], a la luz de cuyas exigencias habrá de enjuiciarse si el grado de formalización y de información en torno a los «criterios de utilización» de los dispositivos digitales (tiempo, modo, frecuencia, contenidos de la información, régimen de acceso, etc.) resulta suficiente; y también, desde luego, exigirse la responsabilidad que proceda en caso de inobservancia. El total incumplimiento de este deber legal, además de ensanchar las posibilidades de imputar responsabilidades al empleador por vulneración del derecho a la privacidad del trabajador –aspecto que no cabe desarrollar en profundidad en estas líneas–, puede también desencadenar relevantes consecuencias de orden procesal. Concretamente, la entrada en juego del artículo 90.4 LJS, en virtud del cual resultará siempre exigible, a nuestro juicio, en ausencia de normas de uso empresarial de los dispositivos electrónicos, la solicitud de

42 En los términos de la STC 241/2012.

43 Pronunciamiento que venía a secundar –e incluso a reforzar– una línea argumental del TEDH (STJUE 3-4-2007, Asunto *Copland*) basada en proclamar la existencia de una expectativa de intimidad que no puede quebrantarse si no se ha advertido previamente al trabajador de que el uso de los dispositivos digitales va a ser objeto de control. Partiendo de ello, el TS vino a efectuar una aportación adicional, al justificar dicha expectativa en la existencia de un hábito social de tolerancia del uso personal, detectando (y completando) quizá una cierta falta de esfuerzo argumental al respecto en la jurisprudencia europea.

44 Para un estudio sistemático de las implicaciones laborales del RGPD (y en particular, de los principios generales de protección de datos), *cfr.* GOÑI SEIN, J. L. 2018: *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa*. Albacete: Bomarzo, especialmente 57 y ss.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

autorización judicial para el acceso a los mismos, a los efectos de la válida obtención de pruebas de sus actuaciones, por ejemplo, a efectos sancionadores[45].

El deber legal de establecer criterios de uso de los dispositivos digitales en la empresa (a través de Códigos de Conducta, Protocolos o instrumentos similares) se somete a un condicionamiento material genérico –sometimiento pleno al marco normativo y a los usos sociales–, al que se añaden otros dos específicos de índole procedimental: los deberes de información a los trabajadores y de participación de sus representantes.

Resulta exigible que tales reglas se formulen de modo claro –nótese el llamamiento legal a la necesidad de establecer «de modo preciso» los usos autorizados, evitando la ambigüedad que se detecta en algunos Códigos actualmente–, y que los trabajadores sean informados de manera adecuada y periódica de la política empresarial contenida en dichos instrumentos, bien directamente, o bien a través de sus representantes[46]. También en este punto, las repercusiones que se derivan de las nuevas exigencias resultan evidentes, al albergar una corrección explícita de los criterios previamente manejados por los tribunales internos: *v. gr.*, por todas, la STS 6-11-2011, en la que se declara la inexistencia de lesión del derecho a la intimidad del trabajador, con motivo del control empresarial del ordenador del trabajador utilizado por el trabajador a través de un «programa espía». A partir de la LOPDPD-GDD, resulta ya indiscutible, por ejemplo, que el empleador tiene que facilitar al trabajador información adecuada sobre

45 En relación con el acceso a los dispositivos digitales, se llegó a plantear hasta qué punto la aparición del artículo 90.4 en la LJS de 2011, destinado a regular la prueba electrónica, podía suponer una derogación de la doctrina del TS que vinculaba el control empresarial a la existencia de normas de uso en la empresa. De sostenerse dicha interpretación, se acabaría privando quizá de relevancia a los Códigos de Conducta. Erigidos estos ahora en un deber empresarial, quizá quepa pensar, como un modo de compaginar las finalidades de ambas normas, en la imperatividad de la intervención judicial siempre que se pretenda efectuar un registro de los dispositivos digitales sin que se hayan formulado previamente reglas de uso según lo ahora preceptuado por el artículo 87.3 LOPDP-GDD, en la línea de las exigencias propias del proceso penal. *Vid.* recientemente STS 23-10-2018 (R. 1674/2018), que decreta la nulidad de la prueba obtenida a través del acceso al ordenador de un directivo despedido y querellado sin autorización judicial, no habiendo advertencia previa de la autorización de un uso exclusivamente profesional. La lectura en clave sistemática o complementaria de ambas normas conduciría así a considerar las previsiones del artículo 90.4 LJS como una suerte de sanción frente a la inobservancia de lo preceptuado en el artículo 87.3 LOPDP-GDD.

46 *Vid.* RCM-CE 2015, apartado 14. El principio de transparencia obliga a informar a los trabajadores de forma correcta, completa y regular: desde la descripción completa de las categorías de datos de carácter personal que pueden ser tratados, hasta las modalidades de control sobre los datos registrados –cuándo y cómo podrán ser realizados–; pasando por la finalidad de la medida de vigilancia, los destinatarios o categorías de destinatarios de la información que se recabe, la duración de retención de la información, su utilización potencial, las copias de seguridad o archivo de los datos recabados y los cauces de ejercicio de sus derechos.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

los programas de control instalados en el ordenador, por lo que no cabe, con carácter general, la instalación de «programas espía», salvo en circunstancias excepcionales en que existan indicios suficientemente fundados de comisión de irregularidades graves por parte del trabajador, y sea esta la única manera de obtener una confirmación o prueba de la misma, y solo durante el tiempo suficiente para la obtención de esta[47].

Más indeterminada resulta la exigencia legal en cuanto al papel que han de desempeñar los representantes de los trabajadores: la ley formula un deber empresarial de propiciar la participación de estos en la elaboración de la política de uso de las TIC en la empresa, pero sin que lleguen a concretarse ni la intensidad ni los términos (formales, temporales, objetivos, subjetivos, modales, etc.) de dicha participación. De este modo, el artículo 87.3 LOPDP-GDD renuncia a otorgar un margen de intervención superior al que garantiza en todo caso, a los órganos de representación unitaria, el artículo 64.5 f) ET: la exigencia de *informe previo* a la ejecución de decisiones empresariales en materia de implantación y revisión de sistemas de organización y control del trabajo. A dicho condicionante procedimental hay que entender que se remite de modo declarativo el precepto, a menos que el convenio colectivo aplicable establezca disposiciones específicas relativas al contenido y/o a las modalidades de ejercicio de los derechos de información y consulta, así como al nivel más adecuado para ejercerlos, siguiendo lo previsto en el artículo 64.9 ET[48]. Sin llegar a albergar un derecho de veto de la representación laboral, como recomienda el WP 29 que se establezca convencionalmente, hubiese sido deseable que la norma contemplase al menos la consulta-negociación como esquema para articular la participación de los representantes de los trabajadores en esta materia, al aportar un refuerzo indiscutible de los principios de licitud, lealtad y transparencia que presiden la regulación reglamentaria (artículo 5.1 RGPD). Aunque no hay que descartar que la implantación de tales reglas de uso pueda, de hecho, albergar, según las circunstancias concurrentes con anterioridad en la organización, una modificación sustancial de condiciones de trabajo de carácter colectivo, en cuyo caso resultaría preceptiva la celebración de un periodo de consultas orientado a lograr un acuerdo colectivo en la materia *ex* artículo 41.4 ET.

La LOPDPD-GDD no contiene, en fin, pronunciamiento alguno sobre si es posible decantarse en la empresa, a la hora de regular los criterios de utilización de los medios

47 *Vid.* para esta conclusión, a partir de Barbulescu II, GOÑI SEIN, J. L.: «La protección de las comunicaciones electrónicas…», *op. cit.*, 25.

48 En esta línea se sitúa, por ejemplo, la recomendación efectuada por el WP 29: el establecimiento, en sede de la negociación colectiva, de previsiones que, superando los derechos de información y consulta de la representación de los trabajadores, condicionen la implementación de los sistemas de supervisión al acuerdo previo de dicha representación en la empresa. *Vid.* WP 29: «Working Document on the surveillance of electronic communications in the workplace», de 29 de mayo de 2002 (WP 55).

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

digitales, por una prohibición total de empleo de los mismos para fines personales[49], como hasta ahora ha venido amparando la jurisprudencia del TS, o sobre si existe un derecho a la utilización de Internet por parte del trabajador[50]. La respuesta a estos interrogantes parece quedar, por consiguiente, remitida implícitamente a los «usos sociales»: un parámetro que, si bien sirve para atender a una realidad social cambiante y casuística, por otra parte, introduce un enorme grado de indeterminación. La posibilidad de efectuar una utilización moderada de los dispositivos digitales en el puesto de trabajo para fines no estrictamente profesionales, que no repercuta en el cumplimiento diligente de las obligaciones laborales ni genere otros perjuicios a la empresa es, a nuestro juicio, la premisa de actuación empresarial que resulta más coherente, en fin, con la función social de la propiedad de los medios de producción *ex* artículo 33 CE: si la propiedad constitucional en general no se compadece bien con una idea de titularidad dominical plena e incondicionada, tampoco parece que la propiedad del empresario sobre los medios digitales haya de ser concebida como un espacio de libertad absoluta de disposición, al margen de su utilidad social[51].

3. EL DERECHO A LA PRIVACIDAD DE LOS TRABAJADORES Y EL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y GRABACIÓN DE SONIDOS

1) *Una premisa esencial ex artículos 22 y 89 LOPDP-GDD: la ilicitud del control directo de la actividad laboral a través de las técnicas de video-monitorización*: El empleo de instrumentos de video-monitorización en el ámbito laboral ha venido limitándose, en

49 Los Códigos de Conducta han venido optando por una de las tres siguientes opciones: 1) la prohibición absoluta del uso de los dispositivos para fines no profesionales; 2) la autorización restringida o limitada del uso personal; o, en fin, 3) la autorización ilimitada de utilización personal; siendo la primera la más extendida. *Vid.* RODRÍGUEZ SANZ DE GALDEANO, B.: «La regulación, mediante Códigos, del uso y control de los medios informáticos y de comunicaciones puestos a disposición del trabajador y de las secciones sindicales». En GOÑI SEIN, J. L. 2011: *Etica empresarial y Códigos de Conducta*. Madrid: La Ley, 370 y ss.

50 Tales cuestiones, suscitadas en su momento por el juez PINTO DE ALBURQUERQUE en su Voto Particular a la STEDH 12-1-2016 (Barbulescu I), se retoman después por parte de la Confederación Europea de Sindicatos en el Recurso ante la Sala General, sin que la STEDH 5-9-2017 (Barbulescu II) se pronunciase finalmente al respecto. El GT 29, por su parte, parecería albergar, implícitamente, en su Documento de 2002 (WP 55) la libre opción del empleador de prohibir a los trabajadores todo uso privado de los dispositivos digitales de la empresa, sin haberse preocupado por alterar dicha posición en los documentos más recientes.

51 *Vid.* MOLINA NAVARRETE, C. 2017: «El derecho al secreto de las comunicaciones en la relación de trabajo: la dilución en "tópica" y "retórica" de su tutela constitucional». *Trabajo y Derecho*, Monográfico, 2017, 6 (www.smarteca.es: 04/12/2018).

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

los textos nacionales e internacionales, a partir de un eje argumental básico: no resulta admisible la puesta en marcha de sistemas de vigilancia y de captación de imágenes con el propósito directo y principal de controlar la actividad y el comportamiento de los trabajadores[52]. Todo ello, sin perjuicio de que su uso en atención a otros objetivos legítimos de la empresa (la protección del sistema de producción, o la preservación de la salud y seguridad de las personas y de los bienes) pueda tener, como consecuencia o efecto indirecto, la posibilidad de monitorizar la actividad del empleado, debiéndose adoptar, en tales casos, salvaguardias adicionales: particularmente la consulta –y en su caso, negociación–, con los representantes de los trabajadores. Resulta lícito, pues, solamente el control indirecto de la actividad laboral a través de instrumentos de videovigilancia, siempre y cuando se garantice, en particular, la íntegra observancia de los principios de protección de datos previstos en el artículo 5 RGPD[53].

Partiendo de lo anterior es como ha de interpretarse el binomio compuesto por los artículos 22 y 89 LOPDP-GDD: este último, de hecho, no es sino un apéndice que asume las coordenadas normativas marcadas por el primero, las cuales resultan de plena observancia en el terreno laboral. Resulta pues infundada cualquier lectura aislada de estos preceptos, que están llamados a ser aplicados no como regímenes alternativos sino cumulativos, pese a la defectuosa literalidad del artículo 22.8 LOPDP-GDD, el cual podría quizá dar a entender indebidamente que se trata de compartimentos-estanco. Antes bien, el tratamiento por el empleador de los datos obtenidos a través de videocámaras previsto en el marco general (artículo 22) se somete (adicionalmente, hay que entender) a las peculiaridades adaptativas dispuestas en el artículo 89 LOPDP-GDD para los entornos laborales. Carecería de sentido, por ejemplo, sostener que no rige en este contexto el deber de supresión de los datos videográficos en el plazo laboral de un mes desde su captación (artículo 22.3), salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de bienes, personas o instalaciones.

Así las cosas, resulta plenamente aplicable en el terreno de las relaciones laborales la premisa básica restrictiva proclamada por el artículo 22.1 LOPDP-GDD: los

52 *Vid.* RCM-CE 2015, apartado 15; así como Opinión de la Comisión de Venecia, órgano consultor del Consejo de Europa, de 8 de junio de 2007, sobre *Videovigilancia por empresas privadas en las esferas pública y privada y por las autoridades públicas en la esfera de lo privado y la protección de los derechos humanos* (apartados 18, 52, 53, 54, 57, 58 y 100); y también el Dictamen 4/2004 (WP 89), de 11 de febrero apartado 8. A nivel interno, *cfr.* Informe AEPD 0533/2006, relativo a cuestiones generales sobre videovigilancia.

53 *Vid.* ampliamente AEPD: *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, elaborada a raíz del RGPD, que enmarca, por cierto, la videovigilancia en los lugares de trabajo en el tratamiento de imágenes con fines de seguridad (pp. 6-27) (www.aepd.es/media/guias/guia-videovigilancia.pdf; 5/02/2019). Para una interesante síntesis, en el ámbito doctrinal, *vid.* CLIZA, C.; OLANESCU, S. y OLANESCU, A. 2018: *Video surveillance: stand point of the EU and national legislation on data protection*. NT University Editorial House, 465-471.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

empleadores podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la *finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones*. El ejercicio esencialmente de un «poder de policía» constituye, por consiguiente, el punto de partida insoslayable para delimitar el marco de desenvolvimiento que corresponde al artículo 89 LOPDP-GDD. El cual, no obstante, remite, acaso de un modo técnicamente cuestionable, al marco jurídico-laboral y a los límites del artículo 20.3 ET, que contempla en cambio facultades ordinarias de vigilancia y control de la actividad laboral. Pese a incurrir en tal incorrección técnica, lo cierto es que 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. Téngase presente, por lo demás, que el control directo ha sido ya expresamente declarado como no amparado por el marco legal del artículo 20.3 ET por parte de la jurisprudencia; por lo que la propia remisión efectuada a éste y a los «límites inherentes al mismo» sirve para llegar a idéntica conclusión interpretativa[54].

2) *El régimen de ejercicio del poder empresarial de videovigilancia y sus límites genéricos:* En el marco, pues, de su dependencia del marco general establecido en el artículo 22, el artículo 89 LOPDP-GDD proclama en su rótulo la existencia de un derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo que, a diferencia de los dos preceptos que le preceden, no es seguido en realidad de una proclamación de tal derecho en el texto del precepto, y menos aún de una delimitación técnica completa de sus perfiles, sino que se concreta más bien en una formulación extremadamente lacónica de los términos que delimitan el ejercicio del poder empresarial de videovigilancia indirecta del trabajo. Se proclama así, con carácter general, su desenvolvimiento dentro del marco legal del artículo 20.3 ET y con los límites inherentes al mismo; lo cual remite hoy día precisamente –y ello nos parece lo más relevante– a la observancia de todos los condicionamientos derivados de la NPD en su conjunto, erigida ahora *ex* artículo 20 Bis ET, en la limitación extrínseca más destacada al poder empresarial de videovigilancia.

Así las cosas, pese a la referencia del precepto al artículo 20.3 ET, lo cierto es que desde el punto de vista de la NPD la base de legitimación para llevar a cabo las medidas a la que se remite el binomio compuesto por los artículos 22-89 LOPDP-GDD

54 *Vid.* SSTS 31-1-2017 (R. 3331/2015); 1-2-2017 (R. 3252/2015); o 2-2-2017 (R. 554/2016). Razones de seguridad en sentido amplio «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*.».

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

es en realidad el *interés legítimo* del empleador a preservar la seguridad y el correcto y ordenado desenvolvimiento de la actividad productiva (artículo 6.1 f) RGPD), quedando subordinada a la consecución de aquel interés la concurrencia de la necesidad del tratamiento para la ejecución del contrato (artículo 6.1 b) RGPD). Ello incide en la proyección del resto de principios relativos al tratamiento de datos: muy especialmente el de la limitación de la finalidad, cuya observancia implica que las imágenes recogidas con una finalidad determinada, explícita y legítima (en este caso, persiguiendo un propósito de control exclusivamente enmarcable en la protección de la seguridad de bienes, personas e instalaciones), no puedan ser tratadas ulteriormente de manera incompatible con dichos fines. Y también, desde luego, la minimización de los datos e imágenes que se capten, que han de ser adecuadas, pertinentes y limitadas a lo necesario en relación con los fines señalados. Y a partir de todo ello, sobre el propio principio de responsabilidad proactiva, que exige que el empleador sea capaz de evidenciar la regularidad de la medida de videovigilancia con carácter previo a su puesta en funcionamiento[55].

En síntesis, ha de acreditarse que la medida de videovigilancia, demostrándose necesaria, se lleve a cabo de la manera menos intrusiva posible y se dirija al área específica donde se manifieste el riesgo. De hecho, resulta inherente a la invocación del «interés legítimo» como título legitimador la contemplación de medidas mitigadoras que aseguren un adecuado equilibrio entre dicho interés y los derechos fundamentales de los trabajadores, tales como, en este caso, la limitación de los parámetros de la medida de videovigilancia (espaciales o geográficos, objetivos, subjetivos, temporales, etc.)[56]. Y, además, ello implicará siempre la existencia, en favor del trabajador, del derecho de oposición al tratamiento sobre la base del cuestionamiento de la base de licitud aportada por la empresa (artículo 21 RGPD). Como punto de partida, antes de la puesta en marcha de un sistema de videovigilancia, el empleador habrá de evaluar previamente si la medida resulta estrictamente necesaria y proporcionada, optando, cuando ello sea posible, por la adopción de otros medios menos intrusivos para la privacidad de los trabajadores[57]. El uso de cámaras o videocámaras no debe suponer un recurso para llevar a cabo una vigilancia defensiva en abstracto, sin un particular

55 En los casos de realización de las funciones de seguridad por una empresa externa, el acceso a las imágenes ha de estar regulado por la existencia de un contrato con un encargado del tratamiento (artículos 28 RGPD y 33 LOPDP-GDD).

56 *Vid.* WP29: Opinión 2/2017, *on data processing at work*, *op. cit.*, 7-8. Igualmente en dicha línea se sitúa, como es sabido, la STEDH 9-1-2018 (López Ribalda y otros c. España I), donde la medida de videovigilancia encubierta sometida a análisis no obedecía a una sospecha fundamentada previa, y, por consiguiente (a diferencia del supuesto previamente analizado en la sentencia Köpke), no estaba dirigida específicamente a un número limitado de empleadas, sino a todo el personal que trabajaba en las cajas registradoras, sin límite temporal y durante todas las horas de trabajo.

57 El uso de cámaras simuladas, por ejemplo, no implica en principio un tratamiento de datos. Si bien en caso de tratarse de cámaras reales desactivadas, o que pueden activarse sin

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

riesgo para la defensa de los intereses patrimoniales de la empresa, o un pretexto para realizar funciones de vigilancia de los trabajadores[58]. Y en todo caso, el control visual constante y permanente de los trabajadores, instaurado en base a una genérica necesidad de seguridad o de protección del patrimonio empresarial, o con el objetivo de verificar posibles conductas ilícitas de los mismos resulta injustificado y manifiestamente desproporcionado, implicando, en realidad, un control directo sobre la actividad laboral de los trabajadores que resultará ilegítimo si no concurre un motivo real de seguridad de carácter excepcional que lo legitime.

Por otra parte, señalar que el principio de minimización será un criterio relevante para enjuiciar, entre otras cuestiones, si el número de cámaras, o el tipo de las mismas (cámaras fijas, cámaras móviles, cámaras «domo» que permiten giros de 360º, etc.) son los adecuados para alcanzar la finalidad perseguida; así como la necesidad, en su caso, de utilizar «máscaras de privacidad» –de tal manera que se evite captar y grabar imágenes excesivas–; o de captar solamente imágenes secuenciadas temporalmente (cada cierto tiempo, etc.)[59].

Los avances tecnológicos en los mecanismos de visualización han venido, en todo caso, a agudizar el potencial intrusivo de la videovigilancia en los entornos laborales: piénsese en la capacidad de acceso a datos recopilados remotamente (*v. gr.*, a través de dispositivos telefónicos, cámaras IP[60] y dispositivos similares); o en la propia reducción del tamaño de las cámaras (paralela al incremento de sus capacidades técnicas y de su resolución). Pero además de afectar a la fase de recopilación de datos *(data collection)*, la tecnología ofrece ahora herramientas de procesamiento ulterior de las imágenes *(data processing)* que habilitan, por ejemplo, al empleador, para el uso de tecnologías de reconocimiento facial: una práctica que ha de reputarse como no

esfuerzos excesivos, deberá aplicarse tanto la NPD como la normativa sectorial que resulte de aplicación: *Vid.* AEPD: «Guía sobre el uso de videocámaras…», *op. cit.*, 49.

58 *Vid.* GOÑI SEIN, J. L. 2018: «Videovigilancia empresarial mediante cámaras ocultas: su excepcional validez como control defensivo "ex post"». *Trabajo y Derecho*, 2018, 47: 75.

59 Junto a ello, es exigible un registro de actividades de tratamiento de datos de videovigilancia que realicen en la empresa, documento interno de la empresa en el que se ha de incluir una descripción simplificada; sin perjuicio de otras posibles exigencias normativas en función de las características particulares del tratamiento de imágenes que se efectúe. *Vid.* AEPD: «Guía sobre el uso de videocámaras…», *op. cit.*, 9 y ss. La evaluación de impacto (artículo 35 RGPD) podrá resultar exigible, por ejemplo, cuando la videovigilancia se establezca para el control de zonas de acceso público a gran escala (Considerando 91 RGPD): *v. gr.*, en grandes centros o establecimientos comerciales.

60 Las cámaras IP, que en ocasiones permiten un control remoto de todas las funciones disponibles en la cámara (zoom, movimiento horizontal, vertical, sonido, etc.), pueden permitir además la visualización de las imágenes desde cualquier ordenador conectado a internet, siempre que no se hayan establecido los debidos controles de acceso, abriendo la vía a posibles brechas de seguridad de los datos videográficos.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

permitida, en principio, al afectar a datos biométricos[61]. Como también resulta ilícito el empleo de aplicaciones diseñadas para captar y analizar las expresiones faciales de los empleados a través de mecanismos de tratamiento automatizado de datos, identificando desviaciones en relación con patrones de movimiento predefinidos (por ejemplo, en el contexto más amplio del centro de trabajo, etc.), o creando perfiles. Con carácter general, a nuestro juicio, el procesamiento ulterior de imágenes de los trabajadores ha de considerarse como una actuación contraria al marco legal vigente.

El binomio compuesto por los artículos 22 y 89 LOPDP-GDD no permite, en suma, la captación de imágenes para propósitos de gestión del empleo en la empresa diversos del control indirecto de los trabajadores vinculados a la preservación de la seguridad; estableciéndose así un trascendental límite extrínseco para el artículo 20.3 ET. Trascendental porque de ello deriva, a nuestro juicio, la inadmisibilidad del empleo de técnicas de videoanálisis de los trabajadores –como manifestación específica, de nuevo, de las técnicas de análisis predictivo y decisional en materia de gestión de los recursos humanos *(Workforce Analytics)*–. Téngase en cuenta, por otra parte, que el principio de limitación de la finalidad implicaría la ilicitud del uso secundario de las imágenes obtenidas en atención a finalidades de preservación de la seguridad, para su tratamiento con otro fin distinto que no resulte compatible: en este caso, fines decisionales en materia de gestión laboral que pueden acarrear consecuencias perjudiciales injustificadas o sesgadas para los trabajadores, y que nada tienen que ver con la posible imputación de actos ilícitos a trabajadores concretos. Siendo los datos biométricos, además, una categoría especial de datos personales, entendemos que las posibilidades jurídicas de justificar su utilización secundaria para dar lugar, por ejemplo, a tratamientos automatizados de datos o a la elaboración de perfiles, también aquí resultan virtualmente inexistentes, a partir de lo dispuesto en el juicio de ponderación regulado en el artículo 6.4 RGPD.

Cuestión distinta es la de la posible validez del comportamiento del trabajador, como base jurídica habilitante para el tratamiento de su imagen, en atención a razones o finalidades totalmente ajenas a la ejecución del contrato de trabajo (*v. gr.*, la difusión en internet de imágenes de la organización y/o del proceso productivo, con la finalidad de reflejar el movimiento y la actividad de la empresa). La grabación de imágenes de los trabajadores con dicho propósito no constituye una facultad contractual del empresario, ni puede confundirse con la facultad de controlar el cumplimiento de la prestación de trabajo, y mucho menos con la seguridad. No obstante, será posible considerar lícitas tales actuaciones, en la medida en que queden amparadas en un otorgamiento expreso y completamente libre del consentimiento del trabajador a su realización, en

61 Solo en casos muy excepcionales, y con fundamento en alguno de los títulos de legitimación específicos del artículo 9.2 RGPD, resultará admisible el empleo de dichas técnicas de reconocimiento facial en las relaciones laborales. *Vid.*, en este sentido, Opinion 2/2017, *on data processing at work*, *op. cit*., 19.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

los términos dispuestos por el artículo 7 RGPD[62], que deben interpretarse además de un modo especialmente restringido en el contexto de las relaciones de trabajo.

3) *El derecho de los trabajadores y de sus representantes a ser informados sobre las medidas de videovigilancia común u ordinaria en la empresa*: La puesta en marcha de medidas de videovigilancia requiere, como elemento condicionante de su licitud, el cumplimiento de deber del empleador de «informar con carácter previo, y de forma expresa, clara y concisa a los trabajadores […], y en su caso a los representantes», acerca de las medidas de videovigilancia. El marco legal se limita, pues, a desarrollar esta concreta faceta del derecho a la privacidad frente al uso de sistemas de videovigilancia: su trascendencia como contenido de los derechos vinculados a la privacidad (artículo 8 TEDH) es el factor que explica, de hecho, que el legislador haya centrado su atención en esta exigencia, de entre todas las que componen el complejo sistema de límites y condicionantes operativos exigibles para la legalidad de las medidas de videovigilancia. Se precisa el alcance de los principios de transparencia y lealtad del tratamiento de datos, a partir del aspecto que ha venido resultando más conflictivo en la experiencia jurídica interna –STC 39/2016, de 3 de marzo (Asunto «Bershka»)–; resultando notorio por otra parte el influjo de la doctrina sentada por la STEDH 9-1-2018 (López Ribalda y otros c. España), correctora de la labor de ponderación llevada a cabo por los tribunales españoles en el caso allí examinado[63].

Por lo que se refiere al alcance objetivo de la información, esta debe concretarse por remisión a lo dispuesto en el artículo 13 RGPD, relativo al deber de información que ha de facilitarse cuando los datos personales se hayan obtenido del interesado[64]. El carácter completo y detallado de dicha información se intenta conciliar con la exigencia de concisión y claridad que preside la filosofía general del RGPD en relación con los principios de licitud, lealtad y transparencia[65]: se contempla así en el marco legal

62 Con anterioridad al RGPD, la AEPD había venido autorizando, de hecho, tal difusión de imágenes de la actividad laboral, estimando que no concurría, en tales supuestos, ninguna de las causas de exclusión del consentimiento previstas en el artículo 6.2 LOPD (Resolución AEPD R/01262/2009, de 2 de junio de 2009). La SAN 24-1-2003, Sala de lo Contencioso-Administrativo, por su parte, excluía la concurrencia de un consentimiento tácito de los trabajadores, por el hecho de soportar pasivamente la captación de imágenes en la redacción de un diario deportivo.

63 *Vid.* CASAS BAAMONDE, M. E.: «Informar antes de vigilar…», *op. cit.*, 115. Información previa que se erige en contenido de los derechos a la vida privada y a la correspondencia (artículo 8 CEDH); y por tanto de los derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de datos de carácter personal.

64 Tal es, de hecho, la indicación a efectos divulgativos efectuada por la AEPD (*v. gr.*, a través de las denominadas «Fichas prácticas de videovigilancia»), en detrimento del marco normativo, de carácter más prolijo y exigente, del artículo 14 RGPD, relativo al deber de información cuando los datos no procedan del propio interesado.

65 *Vid.* Considerando 39 RGPD.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

interno (artículo 11 LOPDP-GDD) la posibilidad de acudir al denominado sistema de «información por capas»[66], consistente en facilitar a los interesados la información básica, complementada por la remisión a una dirección electrónica o a otro medio que permita acceder de forma sencilla e inmediata a la información restante. Dicha información básica deberá, así las cosas, contener al menos los siguientes tres extremos (artículos 11 LOPDP-GDD): a) La identidad del responsable del tratamiento y de su representante, en su caso; b) La finalidad del tratamiento, y c) La posibilidad de ejercer los derechos establecidos en los artículos 15-22 RGPD.

Precisamente el difícil equilibrio que se plantea entre la concisión, claridad y sencillez de la información, y el efecto útil o tutelar de los deberes de transparencia y lealtad, es un factor añadido que acentúa, en el contexto laboral, la necesidad de participación de la representación de los trabajadores. Sobre este particular, no obstante, la LOPDP-GDD se limita a proclamar el deber de informar «en su caso» a los mismos –esto es, siempre que exista tal representación– acerca de la medida en los mismos términos que a los trabajadores. No obstante, resulta también exigible el derecho de la representación laboral de emitir informe con carácter previo a la ejecución empresarial de la medida de videovigilancia, la cual ha de ser considerada como un sistema de control del trabajo *ex* artículo 64.5 f) ET. Un derecho que, entendemos, deberá entrar en juego justamente a continuación del cumplimiento del deber informativo de la LOPDP-GDD: de hecho, resulta esperable que la información suministrada sirva para potenciar tanto la función consultiva como el control de la legalidad de la medida. Siendo criticable la escueta regulación legal, esta conduce en todo caso, a nuestro entender, a una aplicación sucesiva de las garantías informativas dispuestas respectivamente en la LOPDP-GDD y el ET (ampliadas, en su caso, a través de la negociación colectiva), pero no a una anulación de estas por parte de aquellas[67]. Si bien el artículo 64.5 f) ET contiene un trámite procedimentalizador cuya inobservancia no viene dotada de relevancia constitucional (STC 98/2000), su incumplimiento puede desencadenar una pluralidad de consecuencias jurídicas, entre las que conviene destacar el posible ejercicio de acciones jurisdiccionales orientadas a declarar la ineficacia de la medida de videovigilancia empresarial adoptada irregularmente, al regreso a la situación previamente existente y a la remoción de sus efectos en el modo en que se estime más oportuno[68].

66 *Vid.* su presentación en el Preámbulo de la LOPDP-GDD, apartado V.

67 No compartimos, por tanto, la conclusión de que la LOPDPD-GDD haya devaluado la garantía de información-control colectiva, por cuanto que «ni siquiera se respeta el mínimo establecido en el artículo 64 ET»: *vid.* MIÑARRO YANINI, M. 2019: «La "Carta de Derechos Digitales" de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación». *CEF-Trabajo y Seguridad Social*, 2019, 430: 10.

68 *Vid.* MONEREO PÉREZ, J. L. 1992: *Los derechos de información de los representantes de los trabajadores*. Madrid: Civitas, 256-257.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

4) *Videovigilancia extraordinaria y comisión de actos ilícitos por parte de los trabajadores: una habilitación legal para el aligeramiento del derecho de información en los supuestos de control defensivo «ex post»*: La exigibilidad del principio de transparencia en relación con las medidas de videovigilancia ha venido siendo, así pues, el auténtico foco de la conflictividad jurídica en el ámbito interno y europeo. Los términos de la cuestión podrían sintetizarse así: por un lado, resulta esperable que el cumplimiento de los requisitos informativos actúe como mecanismo disuasorio de comportamientos que atenten contra la seguridad de las personas, bienes e instalaciones por parte de cualesquiera sujetos (clientes, público, trabajadores, etc.): la plena consciencia informada por parte de los trabajadores, en particular, de la existencia de mecanismos de control visual, de su utilidad para configurar pruebas demostrativas de conductas irregulares, debería operar justamente como un elemento fundamental en favor de la preservación preventiva de los bienes jurídicos protegidos. No obstante, la exigencia de aquel principio en términos absolutos, especialmente en los casos en los que se haya constatado ya el acaecimiento previo de conductas o actos ilícitos, e incluso quepa dirigir las sospechas sobre su autoría a individuos concretos, acabaría privando de eficacia a tales mecanismos.

Resulta trascendental, en definitiva, a los efectos de interpretar correctamente el artículo 89.1 LOPDP-GDD, efectuar una distinción entre situaciones que son diversas, y que a menudo han venido apareciendo confundidas en el debate doctrinal y jurisprudencial[69]. Efectuar una cierta distinción de supuestos nos parece, así pues, un punto de partida adecuado para orientar concretamente el entendimiento del inciso formulado en el artículo 89.1, segundo párrafo, el cual permite flexibilizar o aligerar los deberes informativos en materia de videovigilancia laboral: «En el supuesto de que se haya captado la comisión flagrante de un acto ilícito[70] por los trabajadores o los empleados públicos, se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta Ley Orgánica».

Y es que la aplicación generalizada e inmatizada de esta previsión normativa a los supuestos de videovigilancia ordinaria (esto es, a la genérica puesta en marcha tales sistemas como mecanismos disuasorios, sin haberse producido previamente quiebra alguna de la seguridad) acabaría vaciando *de facto* el deber general de información en los términos previamente proclamados en el primer párrafo del artículo 89.1, aniquilando completamente la interpretación adaptativa y tutelar de los principios de

69 En este sentido, *vid.* PRECIADO DOMENECH, C. H. 2017: «La videovigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal». *Revista de Derecho Social*, 2017, 77: 184-185.

70 En contraste con la terminología más estricta que se acogía en los textos preparatorios de la norma, la noción de «acto ilícito» comprende obviamente no solo ilícitos de naturaleza penal, sino también incumplimientos graves y culpables sancionables laboralmente, siempre que vayan referidos a la seguridad de los bienes, instalaciones y personas en la organización.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

transparencia y de lealtad efectuados por la norma laboral: la eventual constatación a posteriori de una conducta ilícita acabaría blanqueando o regularizando, de hecho, la puesta en marcha inicialmente irregular de un sistema de videovigilancia sin información previa y expresa a los trabajadores y a sus representantes. Es esta una conclusión interpretativa, carente, en nuestra opinión, de todo fundamento lógico, sistemático y teleológico; por mucho que hubiese sido deseable, desde luego, que el precepto efectuase una clarificación más explícita de la diversidad de supuestos que se plantean.

Es oportuno traer a colación el hecho de que la jurisprudencia del TEDH ha resultado hasta cierto punto permisiva con la posibilidad de establecer controles videográficos ocultos de la actividad laboral, frente a la más dubitativa y oscilante toma de posición al respecto por parte del TC a nivel interno. La STEDH 9-1-2018 (López Ribalda I) vino quizá a situar el debate, de nuevo, más cerca de las coordenadas inicialmente marcadas por TC, al contener un posicionamiento favorable a la videovigilancia oculta, aunque con autorización legal previa y solo en determinadas circunstancias excepcionales[71]. Esta se alinea, en buena medida también con la doctrina de la OIT[72], amparando comportamientos de minoración de la transparencia en atención a la finalidad defensiva de las medidas de videovigilancia y, en concreto, de su utilidad para la verificación por el empleador de la comisión de actos ilícitos por parte de los trabajadores[73]. Una minoración que pasaría esencialmente, según esta atinada construcción doctrinal, por distinguir entre el control dirigido a una generalidad no identificada de empleados (control defensivo *ex ante* y *en abstracto*), y el control individualizado determinado por la existencia acreditada de unos ilícitos previos cometidos por algunos trabajadores

71 Así se deduce nítidamente del contraste entre el supuesto de hecho previamente examinado en la Sentencia *Köpke*, y el examinado en López Ribalda, donde no se siguió una sospecha fundamentada previa específicamente dirigida contra las trabajadoras reclamantes, sino que la medida de videovigilancia tuvo un alcance subjetivo y temporal omnicomprensivo (dirigido a todo el personal que trabajaba en las cajas registradoras, durante semanas, sin límite de tiempo, y durante todas las horas de trabajo, etc.); mientras que en *Köpke*, la medida de vigilancia considerada lícita había sido limitada temporal y subjetivamente (se llevó a cabo durante dos semanas y solo dos empleados fueron objeto de la medida).

72 *Vid.* R. OIT-97: «En cuanto a la vigilancia secreta, sólo es *aceptable en la medida en que esté prevista por ciertas disposiciones de la legislación nacional*. Puede ser indispensable para efectuar investigaciones acerca de actividades delictivas u otras infracciones graves. No obstante […] no basta con sospechar de tales actividades o infracciones. El empleador está autorizado al uso de la vigilancia secreta únicamente cuando existan sospechas razonablemente justificadas de actividades delictivas u otras infracciones graves. Como ejemplo de infracción grave, se menciona el acoso sexual, que puede no ser calificado necesariamente de actividad delictiva» (p. 21).

73 *Vid.* GOÑI SEIN, J. L.: «Videovigilancia empresarial mediante cámaras ocultas: …», *op. cit*., 80, para quien «es obvio que el deber de transparencia no puede amparar ni facilitar al trabajador la comisión de un acto ilícito, y tampoco hacer imposible la comprobación de actos ilícitos. Debe prevalecer el interés público de la sociedad y las salvaguardas contra la ilegalidad».

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

(control defensivo *ex post* y *en concreto*): no todo comportamiento de vigilancia oculta con finalidad defensiva, en suma, debe considerarse, como aceptable, sino solamente los que se enmarquen en el segundo tipo. Lo cual implicaría, por consiguiente, la efectiva comisión de conductas ilícitas previas achacables a un número limitado de sujetos. El control defensivo *ex post* y *en concreto* requeriría así dos cosas: a) la constatación acreditada de una quiebra ya acontecida –y no meramente hipotética– en la seguridad de los bienes e instalaciones del empresario. Y b) aportar sospechas fundadas de comisión del acto ilícito real, previamente acreditado y no meramente hipotético, por parte de un colectivo determinado de personas.

Pues bien, el recurso a esta afinada construcción doctrinal quizá pueda resultar de utilidad para arrojar luz sobre las incertidumbres aplicativas que plantea el artículo 89.1 LOPDP-GDD, partiendo justamente de la necesaria distinción de supuestos que parece requerir su alusión a la «comisión flagrante de un acto ilícito» por parte de los trabajadores. Dicho precepto habría venido así a suministrar una habilitación legal expresa para efectuar, solamente en supuestos excepcionales, un cumplimiento no pleno de los deberes de información que, con carácter general, resultan exigibles en los supuestos de videovigilancia ordinaria[74].

Conviene, en este punto, efectuar una importante precisión: el artículo 89.1 LODPD-GDD, sustancialmente mejorado en este punto durante la tramitación parlamentaria, no contempla una habilitación legal para la vigilancia totalmente secreta, pese a que ello hubiese resultado quizá aceptable a la luz de la jurisprudencia del TEDH y de la propia doctrina de la OIT[75]. A cambio, lo que viene a contemplar es el aligeramiento del deber de información en punto a la detección de la comisión flagrante de actos ilícitos, y, en concreto, para la válida obtención de la prueba correspondiente. La expresión «supuesto de que se haya captado la comisión flagrante de un acto ilícito» debería entenderse, según la interpretación que aquí se propone, referida exclusivamente a situaciones donde, habiéndose ya producido con anterioridad una quiebra de la seguridad en la empresa (existencia previa acreditada de actos ilícitos contra la seguridad de las personas, bienes o instalaciones), existen sospechas fundadas de que su autoría ha

74 Exigencia de habilitación legal expresa apuntada no solo por la STEDH 9-1-2018 (Asunto «López Ribalda») y por la OIT, sino también por el voto particular a la STC 39/2016 (Asunto «Bershka») formulado por los Magistrados Valdés Dal-Re y Asúa.

75 El texto final del artículo 89.1 LOPDP-GDD ha introducido notables mejoras, en comparación con el defectuoso artículo 22.5 del Proyecto de Ley, el cual sí contemplaba la total ausencia de información en caso de apreciarse delitos: «En el supuesto de que las imágenes hayan captado la comisión flagrante de un acto delictivo, la ausencia de información a que se refiere el párrafo anterior no privará de valor probatorio a las imágenes, sin perjuicio de las responsabilidades que pudieran derivarse de dicha ausencia». Un texto que acababa amparando, por otra parte, un notable grado de esquizofrenia legislativa ahora eliminada: la válida obtención de la prueba de un delito podría acabar acarreando consecuencias jurídicas propias de la vulneración de un derecho fundamental, incluida la indemnización de los daños y perjuicios ocasionados.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

podido corresponder a determinados trabajadores. No sería lícita, en cambio, por menoscabar el principio de transparencia, la obtención de una prueba sobre la comisión de un acto ilícito del que no existen precedentes en la empresa, en un panorama, por consiguiente, de ausencia total de sospechas previas.

Efectuando esta interpretación, la LOPDP-GDD vendría incluso a mejorar en este punto los cánones de protección de la jurisprudencia del TEDH: el nuevo marco legal no avala la vigilancia mediante cámaras totalmente ocultas, sino que articula las posibilidades de control defensivo *ex post* y *en concreto* a través del aligeramiento de los deberes informativos. Acaecida una quiebra de la seguridad en la organización, cabe establecer sistemas de videovigilancia que no informen de manera plena a los trabajadores y a sus representantes de todos los extremos legalmente exigidos (artículos 13 RGPD y 11 LOPDP-GDD), sino que bastará, para que la prueba sea válida, con la previa colocación del distintivo informativo en un lugar suficientemente visible, identificando, al menos, la existencia del sistema de videovigilancia, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículo 15-22 RGPD. Dicho control defensivo *ex post* y *en concreto* habrá de someterse igualmente –tal y como exige el TEDH para la videovigilancia totalmente oculta– a criterios de valoración que ponderen las circunstancias temporales y el alcance subjetivo de la medida, siempre dentro del respeto al conjunto de los principios de protección de datos (limitación de la finalidad; minimización, adecuación y pertinencia de las imágenes captadas; exactitud; limitación del plazo de conservación ex artículo 22.3 LOPDP-GDD, etc.).

Se trata de una interpretación viable, y a nuestro juicio equilibrada de la norma, en la medida en que se sigue confiando en el principio de transparencia como instrumento que, en principio, debería resultar eficaz para la disuasión preventiva si se cumplen plenamente las garantías informativas (videovigilancia ordinaria, como medio de control preventivo *ex ante* y en abstracto); al tiempo que se habilita legalmente al empleador para llevar a cabo una minoración de la transparencia (videovigilancia extraordinaria como medio de control defensivo *ex post* y en concreto) orientada a la obtención lícita de pruebas que posibilite la reacción disciplinaria empresarial en caso de que la disuasión genérica no haya existido previamente o no haya resultado efectiva. El marco legal así entendido, pese a no prestar atención a aclarar relevantes cuestiones de índole procesal[76], viene a aportar un mayor grado de seguridad jurídica en torno a la válida

76 La vulneración del principio de transparencia conlleva la obtención de una prueba ilícita (no ya simplemente ilegal), por vulneración de un derecho fundamental, no debiendo aceptarse por el juez sus resultados fácticos, ya se haya practicado esta dentro o fuera de un proceso. Lo cual afectará tanto a los efectos directos como a los indirectos de la vulneración («doctrina de los frutos del árbol envenenado»), estableciéndose una cadena de contaminación en el sentido de que incluso quedarán anulados los resultados de una prueba lícita si esta tiene su origen en la prueba lícita. Sí podrá acreditarse el hecho, en cambio, a través de otras pruebas que no tengan conexión funcional con la vulneración del derecho fundamental. *Cfr.* ampliamente DESDENTADO

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

configuración de la prueba sin incurrir en contradicciones o esquizofrenias reguladoras. Y lo hace cumpliendo con las exigencias constitucionales de habilitación expresa para el recorte de los derechos, a través de una formulación legal que, al no eliminar por completo los deberes informativos, cabe entender también como respetuosa del contenido esencial del derecho a la protección de datos personales (artículo 53.1 CE).

5) *La utilización de sistemas de grabación de sonidos en el lugar de trabajo: su permisividad excepcional, como medida no amparada contractualmente, vinculada al agravamiento del riesgo*: Las técnicas de videovigilancia en ocasiones pretenden ser complementadas mediante el añadido de sistemas de captación y grabación de sonidos. Este aspecto se aborda así en el artículo 89.3, precepto plenamente aplicable, en todo caso, referido a sistemas de captación y grabación de sonidos de carácter autónomo. Contempla aquí la ley un régimen jurídico extraordinariamente restrictivo: se huye de hecho, a diferencia de la videovigilancia, de reconocer el ejercicio de un poder empresarial: el recurso a tales sistemas no se entiende, de hecho, amparado por el marco legal del artículo 20.3 ET, precepto laboral que en ningún momento es aludido por la norma. Ello obliga también quizá a efectuar una interpretación restringida del supuesto de hecho previsto, que se referiría de manera estricta, a nuestro juicio, a la captación de sonidos ambientales en el «lugar de trabajo»: fuera de la órbita del mismo, y plenamente incluibles en el artículo 20.3 ET, quedarían, por ejemplo, supuestos de grabación de conversaciones telefónicas necesarias para la supervisión de la actividad laboral[77], o para la propia preservación de la seguridad de personas, bienes o instalaciones[78]: supuestos quizá excluidos del régimen excepcional *ex* artículo 89.3, pero no de la íntegra aplicación de la normativa general y los principios de protección de datos *ex* artículo 5 RGPD[79].

BONETE, A. y MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, 142-146. Tampoco se pronuncia expresamente el precepto sobre si el régimen de videovigilancia extraordinaria alberga una excepción al principio de jurisdiccionalidad en la adopción de medidas de acceso a documentos o archivos en cualquier tipo de soporte que supongan una vulneración de derechos fundamentales (artículo 90.4 LJS), al resultar ello justificado por razones de eficacia en la obtención de la prueba.

77 *Vid.*, por ejemplo, STSJ Cataluña 26-1-2006 (EDJ 12740), que admite las escuchas telefónicas realizadas en el sector del Telemarketing realizadas aleatoriamente sobre los trabajadores. *Vid.* DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B.: *Control informático…*, *op. cit.*, 28-29. «en el marketing telefónico, si las conversaciones no pudieran ser controladas, la prestación de trabajo tampoco podría ser dirigida y vigilada por el empresario».

78 *Vid.* Informe AEPD 0280/2009, sobre la licitud de las grabaciones de conversaciones de maquinistas ferroviarios con el personal de circulación de las estaciones y entre los propios conductores.

79 *Vid.*, por ejemplo, Informe AEPD 0168/2012, sobre la implantación de un sistema de «mystery shopping» en una red de concesionarios de distribución de bienes de consumo, donde el sistema de control de la calidad se presta por una empresa especializada contratada

© Ediciones Universidad de Salamanca - CC BY-NC-ND

Las grabaciones de sonidos de carácter ambiental, de alcance en principio indiscriminado en el lugar de trabajo, solo resultarán admisibles, así pues, ante la presencia de riesgos «relevantes» o agravados para la seguridad de las instalaciones, bienes y personas derivados, no de cualquier circunstancia, sino de la actividad concreta que se preste en el centro de trabajo. Lo cual no justificará la adopción de cualquier tipo de medida con independencia de su impacto y consecuencias sobre la privacidad de los trabajadores, resultando exigible la observancia estricta de los principios de proporcionalidad y de intervención mínima exigidos por la jurisprudencia constitucional[80]. Junto a lo cual, la norma exige también, como no podía ser de otro modo –aplicación de las garantías previstas en los párrafos anteriores–, el cumplimiento pleno de los deberes informativos previsto para el empleo de los sistemas de videovigilancia: los trabajadores, y también sus representantes, han de ser informados con carácter previo, y de forma expresa, clara y concisa, acerca de la medida de grabación de sonidos en los términos del artículo 13 RGPD y 11 LOPDP-GDD; rigiendo para la representación laboral, a nuestro juicio, el mismo sistema, acumulado y sucesivo, de garantías de información y consulta (información plena + consulta informe *ex* artículo 64.5 f) ET). Todo ello, sin que resulte aplicable ningún tipo de régimen flexible o aligerado de cumplimiento de los deberes informativos.

La base de legitimación para el tratamiento de datos a través de la grabación de sonidos se sitúa así, en definitiva, en el restringido ámbito del «interés legítimo» (artículo 6.1 f) RGPD); en detrimento, ni siquiera de modo indirecto o subordinado, del artículo 6.1 b) RGPD (tratamientos necesarios para la ejecución de un contrato). La ausencia de tal base de legitimación es la que queda reflejada, a la postre, en la falta total de alusión al artículo 20.3 ET. Estas medidas han quedado ubicadas, tras la LOPDP-GDD, fuera de la órbita directiva y fiscalizadora amparada por el contrato de trabajo, y sometidas a un régimen muy estricto de viabilidad jurídica del que ahora se encarga la normativa protectora de la privacidad[81]. De esta decisión legal se deriva, a nuestro juicio, una importante consecuencia, como es la imposibilidad de utilización de los datos personales procedentes de la grabación de sonidos en la empresa con fines de ordenación laboral diferentes de la protección preventiva de la seguridad laboral. Queda vetado, desde luego, el recurso a sistemas de grabación para la obtención de pruebas a efectos

por el empleador que simula acciones comerciales para elaborar informes de calidad; exigiendo el cumplimiento de los deberes de transparencia e información a los trabajadores y a sus representantes.

80 Asume de hecho el precepto los términos literales de la STC 98/2000 («Casino La Toja»), FJ 9.º.

81 Régimen que incluiría, probablemente, la exigencia de una evaluación de impacto de la medida de grabación de sonidos (artículo 35 RGPD), al suponer un tipo de «observación sistemática» del comportamiento, resultando imposible para los trabajadores, en su caso, evitar ser objeto de la misma.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

disciplinarios, sean o no subrepticios. Incluso, por ejemplo, si la existencia de riesgos relevantes para la seguridad de los bienes o instalaciones se justificasen en base a una previa quiebra de seguridad de otros mecanismos preexistentes (*v. gr.*, el fallo previo disuasorio de un sistema de videovigilancia, tomando *a sensu contrario* el razonamiento de la STC 98/2000). Deberá el empresario a nuestro juicio, en caso de corroborarse la posible imputación de actos ilícitos a los trabajadores a través de la captación de sonidos, proveerse de otras pruebas alternativas, dada la falta de amparo de tal técnica de control en el artículo 20.3 ET.

6) *La prohibición en lugares ajenos al desarrollo de la actividad laboral*: Establece el artículo 89.2 LOPDP-GDD, como disposición común tanto para la videovigilancia como para la grabación de sonidos, que «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, tales como los vestuarios, aseos, comedores o análogos». De nuevo el precepto no hace en este punto sino incorporar textualmente una premisa previamente establecida por la jurisprudencia constitucional[82]. De la formulación del TC deriva también el carácter abierto del precepto, cuyas alusiones son meramente ejemplificativas y no taxativas, al referirse genéricamente a cualesquiera lugares ajenos a aquellos donde tiene lugar la ejecución de la prestación laboral: la norma reproduce también, así las cosas, una prohibición absoluta e incondicional de poner en práctica medidas de videovigilancia (y de grabación de sonidos) en lugares distintos de los correspondientes a la ejecución del trabajo que ha resultado cuestionada desde algún sector doctrinal, por resultar excesiva y demasiado general[83].

82 La instalación de tales dispositivos de vigilancia en lugares donde no tiene lugar la actividad laboral resulta «a fortiori, lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias», en tanto que medida empresarial desproporcionada y abusiva. *Vid.* SSTC 98/2000 y 186/2000, que declaran la interdicción de la intromisión del empleador en el ámbito de la esfera privada del trabajador (artículo 18.1 CE), «… que en la empresa hay que entenderlo referido a sus lugares de descanso y esparcimiento, vestuarios, servicios y otros análogos, pero no en aquellos lugares en que se desarrolla la actividad laboral». Con anterioridad, aludiendo al juicio de proporcionalidad, *vid.* también STC 207/1996. En este sentido, debe concluirse que la inobservancia empresarial de la prohibición legal *ex* artículo 89.2 LOPDP-GDD, entre otras posibles consecuencias jurídicas, abrirá la vía de la aplicación de la LO 1/1982, de 5 de mayo.

83 No solo por tratarse de manera igual a lugares cuya relevancia es distinta en términos de impacto sobre la intimidad, sino también por la posible necesidad de someter a control, por motivos de seguridad de las personas o las cosas, lugares ajenos al desempeño del trabajo que son de carácter público: *vid.* DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, 31-33. En esta línea, la STSJ Madrid 14-6-2006 (R. 2640/2006), por ejemplo, consideraba admisible la aplicación de medidas de videovigilancia «débil» en un comedor, sin sistema de grabación ni de captación de sonidos.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

4. EL DERECHO A LA PRIVACIDAD DE LOS TRABAJADORES FRENTE A LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN

La utilización de sistemas de geolocalización (artículo 90 LOPDP-GDD) constituye otro de los escenarios en los que se viene concretando el tratamiento de datos de los empleados en el entorno digital: concretamente, de los denominados datos de localización, que son aquellos que indican la posición geográfica de un determinado equipo o dispositivo electrónico. Puesto que los datos de localización se refieren siempre a una persona física identificada o identificable, constituyen datos personales, entrando en juego la NPD[84]. No en vano, permiten al empresario recabar información sobre los movimientos y el paradero de los trabajadores, bien directamente (localización del propio empleado), o bien indirectamente (localización del vehículo empleado por el mismo, o de un determinado dispositivo u objeto que se encuentre a su cargo); y tanto de una manera temporal como permanente.

Frente a esta amplia fenomenología, que afecta tanto a la línea divisoria entre la vida laboral y la vida privada, como a la determinación de los límites al grado de control y vigilancia laboral que puede llevarse a cabo a través de estas tecnologías, el artículo 90.1 LOPDP-GDD proclama en su rótulo un derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral que, análogamente a lo que sucede con la videovigilancia, no se plasma como tal en el texto del precepto, formulado más bien como el régimen de ejercicio de un poder empresarial[85]. Poder de control que en este caso, no obstante, no viene encorsetado por la estricta finalidad de protección de personas, bienes e instalaciones, como sucede con el régimen de la videovigilancia: no es un poder de policía lo que aquí se disciplina, sino una concreta manifestación del poder de vigilancia y control de la actividad laboral en sentido propio, a través de mecanismos de geolocalización. Una vez más, el carácter lacónico del precepto obliga a reconstruir sus implicaciones llevando a cabo una proyección sistemática de la NPD en su conjunto. Todo ello sin perjuicio, desde luego, de la relevancia de los límites intrínsecos que se presenten frente al ejercicio del poder empresarial de control en cada caso: de modo especialmente relevante, el que el uso fiscalizador de este tipo de tecnologías quede circunscrito a la jornada de trabajo y a aspectos directamente relacionados con la ejecución de la relación laboral, inserta esta siempre en el marco de actividades productivas en las que se presente una necesidad específica de recurrir al tratamiento de este tipo de datos.

84 *Vid.* WP 29: *Dictamen 5/2005 sobre uso de los datos de localización con vistas a prestar servicios con valor añadido*, de 25 de noviembre de 2005 (WP 115), p. 2.

85 El de «tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores […] previstas […] en el artículo 20.3 et», siempre que estas funciones se ejerzan «dentro de su marco legal y con los límites inherentes al mismo».

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

Con carácter general, por consiguiente, estará justificado el control laboral a través del tratamiento de datos de geolocalización cuando el mismo se lleve a cabo formando parte del control del transporte de personas o bienes, o de la mejora de la distribución de los recursos para servicios en puntos remotos –*v. gr.*, la planificación de operaciones en tiempo real–, o bien cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo[86]. No debe considerarse justificado, en cambio, resultando el tratamiento de datos excesivo, en los casos en que los empleados puedan cumplir con sus obligaciones contractuales organizando libremente sus planes de viaje. Y, desde luego, resulta ilícito efectuar tratamientos de datos de localización con el único fin de controlar el trabajo de un empleado, siempre que ello pueda efectuarse por otros medios. Este carácter subsidiario, siempre exigible, se deriva en este caso directamente de la propia base de legitimación que aquí entra en juego, que en este caso remite al artículo 6.1 b) RGPD: tratamientos que resultan *necesarios* para la ejecución de un contrato en el que el interesado es parte[87]; premisa básica que determinará el despliegue de los demás principios del tratamiento: limitación de la finalidad y minimización de los datos en particular[88].

También aquí, como sucede con la videovigilancia, el precepto se limita únicamente a enunciar un solo aspecto del régimen jurídico del ejercicio del poder de control laboral: el deber de los empleadores de informar, con carácter previo y de forma expresa, clara e inequívoca a los trabajadores y a sus representantes «acerca de la existencia y características de estos dispositivos»; así como, igualmente, «acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión». Su lacónica formulación textual resulta criticable, al no hacer alusión al aspecto que más merecería ser resaltado: la finalidad de la adopción de la medida y, concretamente, su posible utilización para la adopción de sanciones disciplinarias. De nuevo aquí, no obstante, una interpretación restrictiva del precepto aferrada a su escueta literalidad, pese a la grave omisión en la que incurre, resulta insostenible desde el punto de vista de la interpretación lógica, teleológica y sistemática. El artículo 90 LOPDP-GDD formula sin duda una pobre y vaga adaptación de los deberes informativos

86 Este es el criterio general tradicionalmente formulado por el WP 29: *Dictamen 5/2005*, *op. cit.*, p. 11.

87 *Vid.*, en este sentido, el previo Informe AEPD 193/2008, resolviendo una consulta genérica sobre el tratamiento de datos emitidos por sistemas GPS en vehículos utilizados por los trabajadores.

88 La Resolución AEPD E/742/2008 se ha ocupado, con carácter general, de delimitar los datos que puede justificadamente recoger un dispositivo GPS para la supervisión de la prestación laboral: la hora de arranque, la hora de aparcamiento, los puntos de paso y las paradas, la velocidad máxima y media de los vehículos, el consumo del vehículo por simulación en función de la distancia recorrida, las horas de funcionamiento, los kilómetros realizados en cada jornada y la desviación de horas del vehículo en función de un horario de trabajo configurable.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

previstos en la normativa general (artículos 13-14 RGPD y 11 LOPDP-GDD); pero sus carencias u omisiones no pueden en ningún caso entenderse como una reducción del alcance general del derecho a la información, lo cual hubiese requerido de la formulación de una habilitación legal de carácter expreso –que aquí ciertamente no concurre– para minorar el contenido esencial del derecho a la protección de datos. El principio de transparencia resulta, pues, plenamente exigible en el contexto del control laboral a través de datos de localización[89], sin que exista aquí previsión legal alguna de carácter expreso que ampare su modulación. De hecho, si no se dispone por parte de los trabajadores de una información plena sobre la medida, que incluya la imprescindible determinación, entre otros extremos, de la finalidad concreta de la medida, el ejercicio de los derechos de reacción por parte del trabajador a los que alude el precepto quedaría materialmente imposibilitado.

Esta lectura de la ley viene a coincidir sustancialmente no solo con la jurisprudencia del TEDH –exigencia general de información previa suficiente siempre que entran en juego los derechos del artículo 8 CEDH–, sino también con el criterio que ha venido manteniendo el Tribunal Supremo[90] y una parte mayoritaria de la doctrina de suplicación hasta la fecha. Debe resaltarse, por cierto, la elevada calidad argumental del razonamiento en una parte sustancial de los pronunciamientos judiciales en punto a la exigencia de los principios de transparencia y de limitación de la finalidad en los

89 Así se resaltaba con nitidez, con anterioridad al actual marco normativo, en el citado Informe AEPD 193/2008, recalcando tanto la exigencia del deber de informar a los trabajadores en los supuestos de geolocalización, pese a no exigirse consentimiento de estos, debiéndose cumplir íntegramente con lo preceptuado en el anterior artículo 5 LOPD, así como el resto de la NPD.

90 El que no exista aún jurisprudencia del Tribunal Supremo dictada en casación para la unificación de doctrina se debe precisamente al hecho de no apreciarse contradicción entre los supuestos sometidos a examen, al fundamentarse todos ellos de manera unánime –pese al distinto sentido de su fallo– en la exigibilidad del deber empresarial de información previa a los trabajadores con alusión expresa a la finalidad de la medida adoptada. *Vid.* ATC 13-9-2016 (RCUD. 2940/2015), que inadmite el recurso porque al trabajador demandante, en una reunión con todos los empleados y la representación de los trabajadores, se le advirtió de que, en el caso de apreciar la existencia de irregularidades en la ejecución de los trabajos en ruta a través de los datos suministrados por un localizador GPS, se procedería a adoptar medidas disciplinarias. Con posterioridad el ATC 19-7-2018 (RCUD. 3945/2017) ha apreciado igualmente falta de contradicción porque, en la sentencia recurrida, la empresa había instalado un GPS de localización de los vehículos adscritos al servicio de una contratación pública, por exigencia del pliego de condiciones de la misma, extremo conocido por el trabajador, encargado del servicio, que elaboraba a su vez partes de vigilancia sobre otros trabajadores. Se resalta así la falta de contradicción con la sentencia de contraste, en la que la empresa incumplió su deber de informar al trabajador de la colocación del dispositivo en el vehículo asignado […], y a su vez el posterior tratamiento de los datos «con una *finalidad completamente distinta de la anunciada*, y por ende, sin conocimiento del conductor».

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

supuestos de control laboral a través de mecanismos de geolocalización[91]. Asumiendo la legítima instalación de mecanismos de geolocalización en aquellas actividades y servicios en los que no puede separarse conceptualmente el control de posición del vehículo de la comprobación del cumplimiento de sus obligaciones por parte del trabajador, la cuestión a resolver sería la de los requisitos a los que debe ajustarse la posible instalación por la empresa de tales sistemas de vigilancia por geolocalización, al fin de salvaguardar el derecho fundamental del artículo 18.4 CE, de cuyo contenido esencial forma parte el derecho de información: si bien esta exigencia informativa no puede tenerse por absoluta dado que cabe concebir limitaciones al derecho fundamental por razones constitucionalmente admisibles y, además, legalmente previstas de un modo expreso. No puede situarse el fundamento de las medidas de geolocalización, por consiguiente, en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia, por cuanto que esa lógica, fundada en la utilidad o conveniencia empresarial, haría quebrar la efectividad del derecho fundamental en su núcleo esencial. Y es que de lo contrario se acabaría confundiendo la legitimidad del fin –la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos– con la constitucionalidad del acto, que exige ofrecer previamente la información establecida por el marco legal como necesaria.

Lesiona el derecho a la protección de datos, en definitiva, el recurso empresarial a medios encubiertos de tratamiento de datos de geolocalización que nieguen al trabajador la información plena exigible por el marco normativo vigente (en la actualidad, artículos 13-14 RGPD y 11 LOPDP-GDD), en el que no se contempla habilitación expresa alguna para su inobservancia; y muy en particular, tal y como ya se venía destacando, que priven de la información necesaria y suficiente a los trabajadores (y ahora también a sus representantes) sobre la instalación de sistemas de geolocalización, sus características y propiedades, y todas las concretas finalidades que con su puesta en marcha se persigue. El marco legal vigente descarta definitivamente, desde luego, la doctrina de la mera conveniencia de la información acogida con escasa fortuna por ciertos pronunciamientos judiciales[92], sin contener previsión legal expresa alguna que

91 En suplicación, partiendo de la doctrina inicialmente sentada por la STSJ Madrid 21-3-2014 (R. 1952/2013), *vid.* también STSJ Castilla-La Mancha 28-4-2015 (R. 134/2015) STSJ Andalucía/Granada 15-7-2015 (R. 1264/2015) o STSJ Andalucía/Granada 19-10-2017 (R. 1149/2017).

92 *Vid.*, por ejemplo, STSJ C. Valenciana 2-5-2017 (R. 3689/2016), cuyo razonamiento aludía a la mera «conveniencia» de haber informado al empleado de la instalación del sistema de geolocalización, como a su carácter de mera «recomendación» por parte del Dictamen 5/2005 del GT 29 de la UE. Valoración que no resiste, por lo demás, el contraste con la literalidad de dicho texto europeo, que subraya nítidamente «la *obligación de informar* a los empleados en cuestión» (p. 12).

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

ampare, ni en general ni en particular, el aligeramiento de los deberes informativos[93]; y además impone la observancia del principio de responsabilidad proactiva, que exige no solo informar detalladamente sobre la existencia y características de los dispositivos y las finalidades de la medida[94], sino también evidenciar, con carácter previo a la implementación de la medida, el cumplimiento integral de los requisitos de licitud impuestos normativamente.

A nuestro juicio, en tanto no se produzca la necesaria aclaración por parte de la AEPD, resulta recomendable en estos casos dar cumplimiento a las obligaciones de transparencia en los términos previstos en el artículo 14 RGPD, marco referido a los supuestos en los que los datos personales no han sido obtenidos directamente del afectado. Así las cosas, el empleador deberá proporcionar a los trabajadores y a sus representantes, con carácter general, la información básica a la que se refieren los artículos 11.2 y 11.3 LOPDP-GDD. Esto es: a) la identidad del responsable del tratamiento; b) la finalidad del mismo; c) la posibilidad de ejercer los derechos establecidos en los artículos 15-22 RGPD; d) las categorías de datos objeto de tratamiento; y e) las fuentes de procedencia de los datos, con especial atención a las características de los dispositivos, según detalla el artículo 90 LOPDP-GDD. Sería recomendable que dicha información básica –que deberá complementarse mediante la indicación de una dirección electrónica u otro medio que permita acceder de manera sencilla al resto de la información exigible–, estuviese disponible mediante circulares informativas o carteles indicativos en todos y cada uno de los vehículos equipados con dispositivos de geolocalización[95]. Todo ello, sin perjuicio del preceptivo cumplimiento individualizado de las obligaciones informativas con cada uno de los trabajadores afectados por la captación de datos de localización, y con sus representantes, a través de modalidades que respeten el contenido normativamente exigible y que permitan al propio empleador demostrar el cumplimiento de las exigencias normativas (firma de protocolos, documentos acreditativos de la recepción de la información, etc.)[96].

93 Se sitúa claramente fuera del marco legal vigente también, por ejemplo, el supuesto contemplado por la STSJ Cataluña 5-3-2012 (R. 5194/2011), que consideraba cumplido el deber de información a partir de declaraciones testificales según las cuales todos los trabajadores conocían la instalación de los dispositivos, porque los mismos emitían un sonido al abrir el vehículo, apagándose al introducir la llave.

94 *Vid.*, por ejemplo, AEPD: Procedimiento AP/00040/2012, sobre vulneración del derecho a la protección de datos por falta de información previa de la instalación de dispositivos GPS en vehículos policiales, en particular, sobre su finalidad de control laboral. O también AEPD: Procedimiento AP/00044/2015, sobre sanción a una Agencia Pública por falta de información previa a sus empleados sobre la instalación de un sistema GPS en los vehículos, al hacerse un seguimiento de las visitas con la finalidad de control laboral.

95 *Vid.* dicha recomendación en el Expediente AEPD n.º E/00597/2006.

96 *Vid.* STSJ Asturias 3-10-2017 (R. 1908/2017), considerando que se cumple con las obligaciones informativas por medio de la remisión al empleado de un documento denominado

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND

Resta señalar, en fin, que quizá otra de las carencias reseñables del precepto, a diferencia del régimen de la videovigilancia, sea la de omitir la determinación de un plazo máximo de conservación de los datos de localización; siendo el plazo de dos meses el que se ha venido recomendando por los textos europeos en la materia[97]. A falta de un pronunciamiento expreso de la norma en este sentido, el plazo de conservación ha de venir marcado, en cada caso, por el principio de limitación de la finalidad: los datos de localización podrán conservarse, a falta de límite normativo específico, tanto tiempo como resulte necesario para la obtención de la finalidad que justifique su tratamiento, si es que no es suficiente al respecto su mera observación en tiempo real, sin recurrir a su almacenamiento. De resultar necesario el tratamiento de datos de localización por un periodo superior a dos meses (*v. gr.*, para elaborar un registro histórico de viajes con el fin de optimizar los recursos), sería recomendable el que previamente se tomase la medida de convertir los datos en anónimos.

«Cláusula de confidencialidad y competencia desleal», que incluía información sobre la posibilidad de efectuar un control remoto a través del GPS de una Tablet entregada como herramienta de trabajo y que el empleado debía mantener operativa durante toda la jornada laboral, advirtiendo de que el incumplimiento de sus disposiciones podría dar lugar a acciones de carácter disciplinario y otras de índole laboral resarcitoria o penal.

97 *Vid.* Dictamen 5/2005 del GT 29, p. 12.

Ars Iuris Salmanticensis,
vol. 7, Junio 2019, 129-171
eISSN: 2340-5155
© Ediciones Universidad de Salamanca - CC BY-NC-ND