



Privacidad y protección de datos de los trabajadores en el entorno digital

Jesús Baz Rodríguez

■ BOSCH



Privacidad y protección de datos de los trabajadores en el entorno digital

Jesús Baz Rodríguez

© **Jesús Baz Rodríguez**, 2019
© **Wolters Kluwer España, S.A.**

Wolters Kluwer

C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
<http://www.wolterskluwer.es>

Primera edición: Septiembre 2019

Depósito Legal: M-29014-2019
ISBN versión impresa: 978-84-9090-397-1
ISBN versión electrónica: 978-84-9090-398-8

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

© **Wolters Kluwer España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

la naturaleza y la finalidad del tratamiento, el tipo de datos personales, las categorías de interesados con alusión explícita a los trabajadores, en su caso, y las obligaciones y derechos del responsable. El marco vigente (artículos 28 RGPD y 33 LOPDP-GDD) se encarga de determinar el contenido mínimo de dicho contrato o acto jurídico, cuyo objetivo será garantizar el cumplimiento de las exigencias normativas de acuerdo con las instrucciones del empleador responsable. Resultará así pues importante la elección de encargados del tratamiento que ofrezcan garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, existiendo un deber de diligencia en la elección del responsable¹⁰⁸.

3.3. 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 en la empresa, además de producirse dentro del marco genérico del artículo 20.3 ET y del sistema de límites recién aludidos que se derivan de la NPD en su conjunto requiere, como elemento central 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 en el trabajo: el derecho de los trabajadores, y de sus representantes, a ser informados con carácter previo y de forma expresa, clara y concisa sobre la puesta en marcha de tales medidas. La especial trascendencia de dicha faceta como contenido de los derechos vinculados a la privacidad (artículo 8 TEDH) es el factor que explica que el legislador haya centrado especialmente su atención en esta concreta exigencia, de entre todas las que componen el complejo sistema de límites y condicionantes operativos exigibles para la legalidad de las medidas de videovigilancia.

El marco legal trata así de precisar el alcance aplicativo de los principios de transparencia y lealtad del tratamiento de datos reconocido en el RGPD en el contexto de la instalación de videocámaras en el ámbito laboral, focalizándose así la atención del precepto, por otra parte, en el aspecto que ha venido resultando más conflictivo en la experiencia jurídica interna. De hecho, se tiene claramente en mente el controvertido precedente de la STC 39/2016, de 3 de marzo (Asunto «Bershka»); resultando igualmente notoria, en la formulación legal, el influjo de los criterios sentados por la STEDH 9-1-2018 (López Ribalda y otros c. España), correctora de la labor de ponderación que había sido llevada a cabo por los tribunales españoles en el caso sometido a consideración.

En apretada síntesis, el debate constitucional mantenido previamente en España sobre el contenido y alcance del principio de transparencia en materia de videovigilancia tiene como punto de arranque la STC 29/2013: partiendo de la centralidad de dicho principio como «elemento caracterizador» y como «núcleo esencial» del derecho fundamental a la protección de datos, esta vino a acoger inicialmente una interpretación

108. *Vid.* Considerando 81 RGPD.

rigurosa del deber de información previsto legalmente (el entonces vigente, artículo 5 LOPD), exigiendo al empresario no sólo la colocación de un cartel distintivo con las indicaciones de la Instrucción 1/2006 de la AEPD (referencia a la LOPD, finalidad del tratamiento e identificación del responsable), sino «la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podía ser dirigida». Interpretación rigurosa sin cuya observancia (información expresa sobre la captación de imágenes, su finalidad de control de la actividad laboral, y sobre la posibilidad de utilizar las imágenes a efectos disciplinarios) resulta ilegítima la utilización con fines sancionadores de las imágenes grabadas. Tal doctrina es la que resultó modificada por la STC 39/2016 (Asunto «Bershka»), al proclamar que la legitimidad de la medida de control audiovisual se podía reconocer sobre la base únicamente de proporcionar información genérica y no específica: la mera colocación por el empleador de un cartel —el distintivo informativo regulado por la Instrucción 1/2006 de la AEPD— anunciando la existencia de cámaras en el lugar de trabajo¹⁰⁹.

La doctrina fijada por la STC 39/2016 venía así *de facto* a sentar la premisa de la prevalencia sistemática del interés empresarial —o más bien incluso, de la mera conveniencia o utilidad— a efectuar controles videográficos, a partir de la habilitación del artículo 20.3 ET, sobre los derechos fundamentales de los trabajadores, en contra del criterio tradicional de la jurisprudencia constitucional¹¹⁰; criterio o canon de constitucionalidad que se acababa sustituyendo, de manera totalmente acrítica, por la interpretación efectuada por un órgano administrativo (la AEPD) sobre la información como elemento esencial del derecho fundamental a la protección de datos. Una cosa es, en suma, la instalación de videocámaras dirigidas al público en general, como colectivo desconocido (clientes, terceros, etc.) —para lo que puede resultar suficiente el cartel anunciador exigido por la Instrucción 1/2006—; y otra situación diferente es la videovigilancia dirigida al personal laboral de la empresa, colectivo bien definido respecto del que el empleador ejerce sus amplios poderes de dirección, control y disciplina de un modo continuado: un marco de actuación del empleador en el cual el deber de información se debe cumplir —como en todos los procedimientos de recogida de datos del

109. La doctrina constitucional sentada en la STC 39/2016 resultaba rechazable, en opinión de un enérgico y autorizado voto particular formulado a la misma, por olvidar que el contenido esencial de los derechos fundamentales, del cual forma parte el derecho de información, constituye «el obligado e imprescindible referente del juicio de constitucionalidad», desembocando inadecuadamente, a partir de ello, en una lógica de ponderación y proporcionalidad para resolver una colisión ficticia de derechos que se desenvuelve, en todo caso, en el terreno de la antijuridicidad, al haberse ejercido los poderes empresariales de manifiestamente fuera del marco legal (artículo 5 LOPD), sin existir ninguna habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales. *Vid.* Voto particular a la STC 39/2016, que formula el Magistrado D. Fernando Valdés Dal-Re, al que se adhiere la Magistrada Adela Asúa.

110. *Vid.* GOÑI SEIN, J.L.: «Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo», *Ars Iuris Salmanticensis*, Vol. 4, 2016, p. 289, quien subrayaba, recordando las SSTC 98/2000 y 186/2000, que «Tiene que haber un interés legítimo y además una estricta observancia del principio de proporcionalidad. Y ese interés legítimo no puede justificarse en la mera utilidad o conveniencia para la empresa».

trabajador por parte del empresario— ajustándose al cumplimiento íntegro de los requerimientos legales.

El incumplimiento de los requisitos de información y transparencia establecidos legalmente sin existir autorización específica en el propio marco legal para ello, y en particular, de la obligación de explicitar previamente, y de informar de manera precisa e inequívoca a los interesados sobre la existencia y las características particulares de un sistema de cámaras —unas visibles y otras ocultas— fue precisamente, en fin, el elemento central, como se sabe, —junto a la inobservancia del principio de proporcionalidad—, en la argumentación de la STEDH 9-1-2018 (López Ribalda I), a la hora de dictaminar que los tribunales españoles no habían logrado un justo equilibrio entre el derecho al respeto de la vida privada y el interés legítimo del empleador a la videovigilancia, constituyendo, en definitiva, la aportación central del TEDH frente a su jurisprudencia anterior¹¹¹. Resulta notoria, así pues, la influencia de dicho pronunciamiento en la aludida decisión de focalizar la caracterización del derecho a la privacidad de los trabajadores frente al uso de videocámaras en esta concreta faceta del derecho: lo cual se produce a través de la afirmación general de un deber empresarial de informar de modo pleno a los trabajadores en los supuestos ordinarios de videovigilancia. Deber que genera el correlativo derecho de los trabajadores y de sus representantes a ser informados en los términos plenos normativamente descritos (artículo 89 LOPDP-GDD incardinado en el marco general del RGPD), como contenido de su derecho a la protección de datos personales.

Por lo que se refiere al alcance objetivo de la información, el deber empresarial de informar «con carácter previo», y «de forma expresa, clara y concisa» a los trabajadores —y en su caso, a sus representantes— sobre el tratamiento videográfico de sus datos personales parece que 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 interesado¹¹². El enriquecimiento de la NPD ha propiciado así un notable ensanchamiento de la información que debe suministrarse, la cual, en síntesis, se proyectaría sobre los siguientes extremos: a) la identidad y los datos de contacto del responsable del tratamiento; b) los datos de contacto del delegado de protección de datos, en su caso, c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento; d) la identificación concreta de los «intereses legítimos» del responsable en que se basa el tratamiento; e) los destinatarios o categorías de destinatarios de los datos personales; f) la intención, en su caso de transferir datos personales a un destinatario a un tercer país; g) el plazo durante el cual se conservarán los datos; h) la existencia del derecho a solicitar el acceso, rectificación, supresión, limi-

111. *Vid.* CASAS BAAMONDE, M.E.: «Informar antes de vigilar...», *op. cit.*, p. 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.

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

tación del tratamiento, oposición y portabilidad de los datos; i) el derecho a presentar una reclamación ante una autoridad de control¹¹³.

Que los destinatarios sean los trabajadores y sus representantes, personas en principio alejadas del conocimiento del sistema normativo de protección de datos, justificaría, hasta cierto punto, la necesidad de conciliar el carácter completo y detallado de dicha información con la exigencia legal de concisión y claridad que preside la filosofía general del RGPD en relación con los principios de licitud, lealtad y transparencia¹¹⁴. Precisamente en atención a la búsqueda preferente de esa concisión se contempla en el marco legal interno (artículo 11 LOPDP-GDD), la posibilidad de acudir al denominado sistema de «información por capas», que había sido ya antes de la LOPDP-GDD aceptado precisamente en ámbitos como la videovigilancia¹¹⁵. Un sistema consistente, en esencia, 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, referida como se ha apuntado al marco general del artículo 13 RGPD, deberá, así las cosas, contener al menos los siguientes tres extremos, en base a lo dispuesto en el artículos 11 LOPDP-GDD:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.
- c) La posibilidad de ejercer los derechos establecidos en los artículos 15-22 RGPD.

El marco normativo interno trata así de hallar un delicado —y en la práctica a veces dificultoso— punto de equilibrio entre las necesidades concisión, claridad y sencillez, por un lado; y el efecto útil y tutelar de la información como contenido de un derecho extremadamente complejo en su diseño normativo como es el de la protección de datos personales. No en vano, la denominada «información básica», en este contexto, bien puede suponer una devaluación o banalización del deber de transparencia informativa, al limitarse exclusivamente a los tres extremos citados. Nada prevé el RGPD, desde luego, como se apuntó más atrás, sobre la posibilidad de clasificar la información en diferentes niveles, por lo que resulta cuando menos cuestionable que la normativa interna pueda efectuar esta particular interpretación de aquél. Así las cosas, el «efecto útil» de la información ofrecida ha de ser, en todo caso, el parámetro de valoración al que ha de acudirse para calibrar el grado de cumplimiento efectivo de los deberes de transparencia y lealtad que se derivan del RGPD, a través del sistema de información por capas dispuesto en la normativa española. De manera particularizada en el terreno

113. Se excluyen aquí ciertas informaciones enumeradas en el artículo 13 RGPD que no resultan procedentes, tales como si el tratamiento de datos personales es un requisito legal o contractual; o la existencia de decisiones automatizadas, incluida la elaboración de perfiles; o la proyección de un tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron. Estas dos últimas cuestiones se refieren a prácticas, en principio, inadmisibles de tratamiento de datos videográficos de los trabajadores.

114. *Vid.* Considerando 39 RGPD: «El principio de transparencia exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro».

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

de la videovigilancia laboral, ello conduce a la exigencia, a nuestro juicio, de un grado de detalle elevado en cuanto a la especificación tanto de la finalidad del tratamiento (utilización de las imágenes para la detección de robos, irregularidades, sustracciones, identificación de sujetos responsables, imposición de sanciones, etc. como de la modalidad técnica de videovigilancia empleada (ubicación y características del sistema de captación de imágenes, sistemas de supervisión y almacenamiento en su caso de las mismas, etc.).

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 la necesidad de participación de la representación de los trabajadores en los supuestos de puesta en marcha ordinaria de los sistemas de videovigilancia laboral. Sobre este particular, no obstante, la LOPDP-GDD se limita en el artículo 89 a proclamar el deber de informar «en su caso» a los representantes de los trabajadores (entiéndase, referido a las situaciones en que tales representantes existan) acerca de la medida de videovigilancia exactamente en los mismos términos que a los trabajadores: esto es, con carácter previo y de forma expresa, clara y concisa. Se habilita a la empresa para poder recurrir, por consiguiente, también en el plano colectivo, al sistema de información por capas contemplado en el artículo 11 LOPDP-GDD, sin prever ningún procedimiento o cauce de consulta-negociación, como recomiendan los documentos internacionales (Consejo de Europa, OIT, etc.).

No obstante, justamente a continuación del cumplimiento de dicho deber informativo, tendrá lugar la entrada en juego del derecho de la representación laboral de emitir informe (consulta-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. Una vez facilitada la información básica a la representación laboral, el empleador habrá de concederle a la misma, así pues, un plazo temporal suficiente a los efectos de que esta pueda emitir el informe previsto en la normativa estatutaria. De hecho, resulta esperable que los deberes informativos de la LOPDP-GDD hayan de servir para potenciar tanto el control de la legalidad de la medida como la función consultiva del informe previo previsto en la normativa laboral: la correcta observancia del derecho de información por parte del empleador ha de servir justamente para que la representación laboral adquiera el cabal conocimiento de la medida de videovigilancia ordinaria que se pretende poner en práctica. El criticable abstencionismo de la LOPDP-GDD conduce, así pues, en todo caso, a una aplicación sucesiva en el tiempo 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 éstas por parte de aquéllas¹¹⁶. Un trámite de consulta-informe cuya exigibilidad

116. Resultando criticable la falta de ambición de la LOPDPD-GDD en cuanto al fortalecimiento del control colectivo de la representación laboral en materia de videovigilancia, no compartimos, en cambio, 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.: «La «Carta de Derechos Digitales» de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación», *CEF— Trabajo y Seguridad Social*, n° 430, 2019, p. 10.



La presente obra ofrece un análisis de la problemática jurídica planteada por el tratamiento de datos personales de los trabajadores por parte de las empresas en vías de transformación digital, en un entorno caracterizado por la creciente digitalización y datificación de la gestión del empleo en las organizaciones. Partiendo del derecho a la protección de datos personales y de su renovado marco jurídico europeo e interno (Reglamento General de Protección de Datos y Ley Orgánica 3/2018), se examinan las principales implicaciones del nuevo conjunto normativo en este particular contexto, en el que el legislador interno ha dispuesto un marco embrionario de garantía de los derechos digitales laborales en situaciones como el uso de dispositivos digitales en el ámbito laboral, la videovigilancia y la grabación de sonidos o la utilización de sistemas de geolocalización. La obra aborda, además, el análisis jurídico de otros escenarios relevantes en los que se efectúa igualmente una recogida de datos personales (uso de dispositivos digitales móviles o situados fuera de los lugares de trabajo, tratamiento de datos biométricos, tratamiento de datos procedentes de las redes sociales, sistemas de denuncias internas, etc.). Finalmente, se analiza el recurso a las técnicas analítico-decisionales en el ámbito laboral y la transferencia de datos personales de los trabajadores en los grupos empresariales y uniones de empresas.

ISBN: 978-84-9090-397-1



9

788490

903971



3652K281760



ER-0290/2005



GA-2005/0100