



Revista del Ministerio de Trabajo y Economía Social

Derecho del trabajo



GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL

148

2021

Revista del Ministerio de Trabajo y Economía Social

Derecho del Trabajo

CONSEJO ASESOR

- Serie Derecho del Trabajo: **Joaquín García Murcia**, Catedrático de Derecho del Trabajo y Seguridad Social. Universidad Complutense de Madrid. **Yolanda Valdeolivas García**, Secretaria de Estado de Empleo.
- Serie Seguridad Social: **Julia López López**, Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad Complutense de Madrid. **Borja Suárez Corujo**, Director General de Ordenación de la Seguridad Social.
- Serie Derecho social Internacional y Comunitario: **Luís Enrique de la Villa Gil**, Catedrático Emérito de Derecho del Trabajo y de la Seguridad Social. Universidad Autónoma de Madrid. **Marcos Fraile Pastor**, Subdirector General de Relaciones Internacionales Sociolaborables.
- Serie Economía y Sociología: **Gerardo Meil Landwerlin**, Catedrático de Sociología. Universidad Autónoma de Madrid. **Raquel Peña Trigo**, Vicesecretaria General Técnica.
- Serie Migraciones Internacionales: **Emiliano García Coso**, Decano Asociado Internacional del Centro de Estudios Superiores Sergio Arboleda, adscrito a la Universidad Rey Juan Carlos. Profesor de Derecho de la UE. **Pilar González Puente**, Directora del Gabinete Técnico de la Secretaría General de Inmigración y Emigración.

COMITÉ DE EVALUACIÓN EXTERNO

Maximino Carpio García, Catedrático de Hacienda Pública. Universidad Autónoma de Madrid.

María Antonia Castro Arguelles, Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad de Oviedo

Ángel Antonio Blasco Pellicer, Magistrado del Tribunal Supremo. Sala Cuarta.

Cristina Gortazar Rotaeche, Titular de la Cátedra Jean Monnet de Derecho de la UE. Universidad Pontificia de Comillas-ICADE.

Nuria Paulina García Piñeiro, Profesora Titular de Derecho del Trabajo y Seguridad Social. Facultad de Derecho. Universidad Complutense de Madrid.

DIRECTORA

Blanca Cano Sánchez
Secretaria General Técnica

SUBDIRECTOR

Luis Navas López
Subdirector General de Informes,
Recursos y Publicaciones

SECRETARÍA

Subdirección General de Informes, Recursos y Publicaciones
del Ministerio de Trabajo y Economía Social

Agustín de Bethencourt, 11

28003 Madrid

Telfs: 91 363 23 05

91 363 23 05 / 03

Fax: 91 363 23 49

Correo Electrónico: proproeditorial@mites.gob.es

Internet: <https://www.mites.gob.es/es/revistaministerio/>

La Revista del Ministerio de Trabajo y Economía Social
no se responsabiliza de las opiniones expresadas
por los autores en la redacción de sus artículos.

Se permite la reproducción de los textos siempre que se
cite su procedencia.

RET: 21-2.387

Catálogo de publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>



Edita y distribuye:

Ministerio de Trabajo y Economía Social
Subdirección General de Informes,
Recursos y Publicaciones

Agustín de Bethencourt, 11. 28003 Madrid

NIPO Papel: 117-20-031-8

NIPO PDF: 117-20-033-9

ISSN Papel: 2660-4647

ISSN Electrónico: 2660-4655

Depósito legal: M-12.168-1998

Diseño cubierta: CSP

Diseño interior: C & G

Imprime: Estilo Estugraf Impresores, S.L. • Telf. 91 808 62 00

Revista del Ministerio de Trabajo y Economía Social

Derecho del Trabajo

PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA
DE LOS DERECHOS DIGITALES EN EL ÁMBITO LABORAL

SUMARIO

EDITORIAL, *Joaquín García Murcia*, 9

ESTUDIOS

El marco jurídico de la protección de datos personales: Reglamento
UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre.

Antonio Troncoso Reigada, 23

El derecho a la protección de datos personales: configuración y relación
con otros derechos de la persona. *Juan José Fernández Domínguez*, 65

Contenido y elementos principales al derecho de protección de datos.

María Belén Cardona Rubert, 97

Recogida y tratamiento de datos personales en el contexto del
contrato de trabajo. *Alberto Cámara Botía*, 113

Categorías especiales de datos personales en el ámbito de la relación
de trabajo. *Ángel Luis de Val Tena*, 143

Protección de datos personales y procesos de selección de trabajadores.

Olga García Coca, 187

Sistema de denuncias y protección de datos personales.

Rosario Cristóbal Roncero, 213

Facultades empresariales y garantías del trabajador en relación con el uso de dispositivos digitales en el ámbito laboral. *Federico Navarro Nieto, 235*

Videovigilancia laboral y grabación de sonidos en el lugar de trabajo.

Jesús Lahera Forteza, 261

Utilización de sistemas de geolocalización en el ámbito laboral. *Iván*

Antonio Rodríguez Cardo, 283

Derecho a la desconexión digital en el ámbito laboral. *Carolina San Martín*

Mazzucconi, 325

Protección de datos personales y garantía de derechos digitales en el empleo público. *Ferrán Camas Rodas, 351*

Registro de jornada de trabajo y protección de datos personales.

Ana Belén Muñoz Ruiz, 377

Gestión y aplicación empresarial de las exigencias sobre protección de datos personales. *Eva María Blázquez Agudo, 399*

El papel de la negociación colectiva en el terreno de la protección de datos personales y garantía de los derechos digitales.

Raquel Yolanda Quintanilla Navarro, 431

Recogida y tratamiento de datos personales en el contexto del contrato de trabajo

Collection and processing of personal data in the context of the employment contract

ALBERTO CÁMARA BOTÍA*

1. INTRODUCCIÓN: EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, UNA DIMENSIÓN INSEPARABLE DE LA RELACIÓN LABORAL

El derecho fundamental a la protección de datos¹ (arts. 18.4 CE, 8 CD-FUE y 16.1 TFUE), que atribuye a las personas un poder de disposición y de control sobre sus datos personales (STC 292/2000, de 30 de noviembre [FJ 7]²), en-

cuentra una de su más importantes aplicaciones en el ámbito de la relación laboral³.

Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele" (FJ 7). Véase SAN MARTÍN MAZZUCCONI, C.: "El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en SAN MARTÍN MAZZUCCONI, C. (Dir.): *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, León, Eolas, 2014, pp. 211 a 213.

³ GARCÍA MURCIA, J.; RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216 (2019), p. 9 (versión electrónica). TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010, p. 1 (citado según la versión electrónica del capítulo 13 del libro ["La protección de datos personales en el ámbito laboral"], TOL2.029.308).

* Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Murcia.

¹ Sobre su formación y configuración, OLLERO TASSARA, A.: *De la protección de la intimidad al poder de control sobre los datos personales*, Madrid, Real Academia de Ciencias Morales y Políticas, 2008, pp. 137 a 168.

² El amplio contenido de este derecho fundamental queda descrito en la STC 292/2000, de 30 de noviembre: "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Su ciclo vital (selección, contratación, cumplimiento y extinción) permite disponer de una información masiva sobre el trabajador, de un elevadísimo número de datos personales sobre sus más variadas circunstancias⁴: identificación, localización, aptitud, formación, salud, afiliación sindical, situación familiar, horario, rendimiento, salario, relaciones humanas, etc. No resultará extraño, por tanto, afirmar que la normativa sobre protección de datos personales se ha convertido en una dimensión inseparable de la puramente laboral⁵. En este sentido se ha señalado que la “legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo” y éste, a su vez, “no puede aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos”⁶. O dicho de otro modo, que buena parte del Derecho del Trabajo puede ser mirado desde el singular punto de vista proporcionado por el derecho fundamental a la protección de datos personales, conforme al cual el empresario aparece como responsable del tratamiento⁷ y el trabajador como interesado⁸, alineándose de modo inescindible con la relación laboral otra derivada de la vigencia del derecho a la protección de datos. Esta afirmación puede sustentarse en las siguientes bases:

- 1.º Sería imposible la celebración, cumplimiento y extinción del contrato de trabajo sin la disposición de datos

⁴ RODRÍGUEZ ESCANCIANO, S.: “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Revista de Trabajo y Seguridad Social CEF*, núm. 423 (2018), p. 22.

⁵ Como señala MARTÍNEZ MOYA “la transversalidad del derecho fundamental a la protección de datos tiene su claro reflejo en las relaciones laborales”. MARTÍNEZ MOYA, J.: “El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores”, *Revista de Jurisprudencia Laboral*, núm. 1 (2019), p. 8.

⁶ Dictamen 8/2001, sobre el tratamiento de datos personales en el contexto laboral (13.9.2001), adoptado por el Grupo de Trabajo del Artículo 29. Citado en el Informe 0529/2009 de la AEPD de donde se toma.

⁷ Art. 4.7 RGPD.

⁸ Art. 4.1 RGPD.

personales de los trabajadores⁹. Más aún, “muchas actividades realizadas de forma rutinaria en el ámbito del empleo implican el tratamiento de datos personales de los trabajadores”¹⁰. Esto es así porque siendo el de trabajo un contrato personalísimo en el que su objeto, el trabajo, es inseparable de la persona que lo presta, su celebración, cumplimiento y extinción exigen mantener un flujo de datos personales en diferentes direcciones: del trabajador al empresario y de éste a aquél¹¹; del empresario a la administración laboral y a los representantes de los trabajadores; de los representantes de los trabajadores a los trabajadores representados. Recogida y tratamiento de datos que unas veces vendrá exigida por la propia “naturaleza de las cosas” (¿cómo se podría celebrar un contrato sin disponer de los datos de los contratantes?), otras por las leyes que obligan a comunicar datos personales, y otras, por no alargar más la enumeración, por el interés y conveniencia del empresario que, por ejemplo, usa instrumentos de control del personal que conllevan necesariamente el tratamiento de sus datos personales.

- 2.º Todos los actos anteriores suponen la disposición del derecho fundamental a la protección de datos, un capítulo más del tema de la vigencia de los derechos fundamentales inespecíficos del trabajador en el contrato de trabajo, pues como se viene afirmando, “la celebración de un contrato de trabajo no implica en modo alguno

⁹ GARCÍA MURCIA, J.: “La protección de datos personales en el ámbito laboral: una sucinta reseña jurisprudencial a partir de cinco sentencias del Tribunal Supremo”, *Revista Galega de Dereito Social*, núm. 5 (2018), p. 10.

¹⁰ Dictamen del Grupo de Trabajo del artículo 29 (8/2001), sobre el tratamiento de datos personales en el contexto laboral.

¹¹ Un ejemplo bien significativo: Art. 8.3 ET.

la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano. Ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad ni la libertad de empresa que establece el art. 38 del texto constitucional legitima el que quienes prestan servicios en aquélla por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional” (STC 88/1985, de 19 julio [FJ 2]).

- 3.º De los dos elementos anteriores, necesidad del tratamiento de datos personales para el desenvolvimiento de la relación laboral y atribución al trabajador de un poder de disposición y de control sobre los mismo configurado como derecho fundamental, resultará la modulación del derecho fundamental a la protección de datos. Así sucede con carácter general cuando se confrontan los derechos fundamentales del trabajador con los del empresario (arts. 33 y 38 CE)¹² o de otros sujetos (art. 28.1 CE) que también pueden tener interés legítimo en el acceso a datos personales de los trabajadores. Lo peculiar del derecho a la protección de datos es que el equilibrio con otros derechos fundamentales no queda remitido sólo a la ponderación judicial, sino que cuenta con una importante regulación legislativa que ya la ha efectuado: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por

el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD)¹³.

El derecho fundamental a la protección de datos personales se convierte así en un punto desde el que el Derecho del Trabajo, y particularmente el contrato de trabajo, puede ser mirado en su integridad¹⁴. A la luz de este derecho fundamental, entre el trabajador, como “interesado”, y el empresario, como “responsable del tratamiento” de los datos personales, se anudan un complejo conjunto de derechos y obligaciones. De ese amplio conjunto de obligaciones y derechos corresponde a este trabajo el estudio de la recogida y tratamiento de datos personales en el contexto del contrato de trabajo. Ese contexto, amplísimo, de algún modo resulta definido en el art. 88 RGPD: contratación de personal; ejecución del contrato; 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 o clientes; efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo; extinción de la relación laboral. Obviamente no se va a estudiar en este artículo toda la problemática que plantea la recogida y tratamiento de datos personales en el contrato de trabajo, por cuanto en otros estudios de este mismo número de la *Revista del Ministerio* se analizan los aspectos específicos del derecho analizado: la protección de datos en los procesos de selección de personal; el tratamiento de de

¹² STC 90/1997, de 6 mayo (FJ 4).

¹³ Deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (en adelante, LOPD-1999).

¹⁴ A la “reinterpretación del conjunto del Ordenamiento jurídico en clave de protección de datos” alude R. MARTÍNEZ MARTÍNEZ: “El derecho fundamental a la protección de datos: perspectivas”, *Revista de Internet, Derecho y Política*, núm. 5 (2007), p. 52.

las categorías especiales de datos personales a las que se refiere el art. 9 RGPD (datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física); la protección de datos y el registro de la jornada de trabajo; denuncias internas (art. 24 LOPDGDG); o, en fin, el estudio de los derechos digitales expresamente nominados en la LOPDGDG: intimididad y uso de dispositivos digitales (art. 87), desconexión digital (art. 89); intimididad frente al uso de sistemas de videovigilancia y grabación de sonidos (art. 89); sistemas de geolocalización (art. 90); o al papel de la negociación colectiva en la protección de datos (art. 91). También, por supuesto, se estudian en otros artículos de este volumen los aspectos generales del derecho: marco normativo, configuración y contenido del derecho. Por tanto, para evitar innecesarias y tediosas reiteraciones, se ha optado por presentar en estas páginas, siguiendo la ordenación sistemática habitual¹⁵, una sucinta reseña de la casuística más destacada que ha planteado la recogida y tratamiento de datos en el contexto del contrato de trabajo¹⁶.

2. RECOGIDA Y TRATAMIENTO DE DATOS EN LA CELEBRACIÓN DEL CONTRATO DE TRABAJO: CONSENTIMIENTO DEL TRABAJADOR, EJECUCIÓN DEL CONTRATO Y CUMPLIMIENTO DE OBLIGACIONES LEGALES

2.1. Tratamiento de datos personales necesario para la ejecución del contrato y consentimiento del trabajador

La celebración del contrato de trabajo es un momento en el que se concentra de modo importante la recogida y tratamiento de datos personales de los trabajadores. El mismo contrato de trabajo puede ser instrumento útil para el cumplimiento de dos importantes funciones: recabar el consentimiento del trabajador para el tratamiento de datos [art. 6.1.a) RGPD] e informarle sobre el tratamiento realizado [arts. 12 y 13 RGPD]. Respecto de los datos que el empresario puede recabar hay que estar al principio de “minimización de datos”: los datos personales han de ser “recogidos con fines determinados, explícitos y legítimos” [art. 5.1.b) RGPD] y “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados” [art. 5.1.c) RGPD].

Basta leer un formulario de contrato de trabajo para apreciar el importante número de datos personales que requiere su formalización: nombre y apellidos, número de documento nacional de identidad, fecha de nacimiento, número de afiliación a la Seguridad Social, nacionalidad, domicilio y nivel formativo. Además en función de la clase de contrato de que se trate podrán exigirse otros datos relativos a situaciones personales del trabajador: discapacidad, desempleo, exclusión social, víctima de violencia de género, de terrorismo o de trata de seres humanos y grado de parentesco con el empresario. Son datos que se encuentran bajo el poder de disposición y control del trabajador cuyo tratamiento resulta absolutamente necesario para la celebración

¹⁵ DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Valladolid, Lex Nova, 2012, pp. 90 a 92. RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009, pp. 9 a 15. PRECIADO DOMENECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Cizur Menor (navarra), 2017. MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª ed., Madrid, Lefebvre, Madrid, 2019. GARCÍA MURCIA; RODRÍGUEZ CARDO: *cit.*, p. 9.

¹⁶ Sobre la recogida y tratamiento de datos en el contexto de las relaciones colectivas de trabajo véase MERCADER UGUINA, J. R.; DE LA PUEBLA PINILLA, A.: “Protección de datos y relaciones colectivas”, *Revista de Trabajo y Seguridad Social. CEF*, núm. 423 (2018).

del contrato de trabajo. Por tanto la licitud de su recogida y tratamiento se encuentra en la regla del art. 6.1.b) RGPD: el tratamiento será lícito si “es necesario para la ejecución de un contrato en el que el interesado es parte”. Como ha señalado la STC 39/2016 “en el ámbito laboral el consentimiento del trabajador pasa [...] como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes”. No es necesario, por tanto, recurrir al principio del consentimiento del interesado [art. 6.1.a) RGPD] para hacer lícito el tratamiento de estos datos indispensables para la celebración y posterior ejecución del contrato de trabajo. Igual régimen que los datos citados anteriormente tendrían otros, también necesarios para el cumplimiento de obligaciones empresariales durante el desarrollo del contrato de trabajo, que se suelen recoger en el momento de la celebración del contrato como sucede con la cuenta bancaria para el abono del salario (art. 29.4 ET)¹⁷.

Más allá de los datos personales necesarios para la ejecución del contrato de trabajo puede que el empresario tenga interés en acceder a otros que no son necesarios pero cuya recogida y tratamiento puede resultarle conveniente. Así sucedería con datos personales de muy frecuente uso en el trato social como son la dirección particular de correo electrónico y el número del teléfono privado que, salvo excepciones, no son necesarios para el cumplimiento del contrato de trabajo. En estos casos la única fuente de licitud del tratamiento de estos datos sería el consentimiento del trabajador, por lo que resulta pertinente plantear cuáles serían los requisitos de una válida prestación de consentimiento del trabajador para ser considerada una “manifestación de voluntad libre, específica, informada e

inequívoca” del interesado (art. 4.11 RGPD). La normativa sobre protección de datos personales contempla con muchas limitaciones y cautelas la prestación del consentimiento del interesado en el mismo contrato para el tratamiento de datos que no están necesariamente relacionados con su celebración y cumplimiento. La razón de estas precauciones es clara: se trataría de una cláusula inseparable del mismo contrato, de modo que el trabajador lo acepta o lo rechaza íntegramente. La aceptación del empleo va unida a la del tratamiento de esos datos personales que no están relacionados con el mantenimiento del contrato: o lo toma todo o lo deja todo. En una relación como la laboral, de posiciones asimétricas y de debilidad contractual del trabajador, se podría afirmar que el consentimiento para el tratamiento de esos datos personales dista de haber sido prestado en condiciones de plena libertad¹⁸. En este sentido las *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* del Grupo de Trabajo del artículo 29 sobre Protección de Datos afirman que “dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas”¹⁹.

¹⁸ De “fuerza o compulsión económica” habla VILLALBA SÁNCHEZ, A.: “El derecho fundamental a la protección de datos del trabajador frente a los riesgos de la contratación estandarizada”, *Nueva Revista Española de Derecho del Trabajo*, núm. 207 (2018), p. 105. SÁNCHEZ QUIÑONES, L.: “El marco legislativo de la protección de datos en el ámbito laboral. Especial referencia al consentimiento del trabajador”, *Diario La ley*, núm. 9377 (2019), (versión electrónica La Ley 2789/2019).

¹⁹ Dice así el citado documento: “También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar

¹⁷ SEMPERE NAVARRO, A. V.: “El deber de facilitar una cuenta corriente bancaria”, *Revista de Jurisprudencia Laboral*, núm. 7 (2019).

El propio RGPD recoge esta problemática en su art. 7.4 RGPD cuando dice que para evaluar si el consentimiento se ha prestado libremente “se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato”²⁰. De igual modo conforme al art. 6.3 LOPDGD “no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”.

impresos de evaluación, sin sentirse presionado a dar su consentimiento.

Por tanto, el GT29 considera problemático que los empleadores realicen el tratamiento de datos personales de empleados actuales o futuros sobre la base del consentimiento, ya que no es probable que este se otorgue libremente. En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [artículo 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado.

No obstante, esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas”. COSTA, R.: “Protección de datos en el ámbito laboral”, en RALLO LOMBARTE, A.: *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019, p. 7 [versión electrónica TOL7.218.410].

²⁰ El considerando 43 del preámbulo del RGPD señala que “para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento”.

Se trata de una cuestión que ha dado lugar a una cierta litigiosidad en la que se puede apreciar dos grandes grupos de casos. Uno en el que los datos personales para cuyo tratamiento se presta el consentimiento no guardan relación con el objeto del contrato de trabajo y otro en el que los datos personales sí están implicados en la prestación laboral del trabajador. En el primer caso no se considera válida la prestación del consentimiento, en el segundo sí. Dentro del primer grupo la STS de 21 de septiembre de 2015 (rec. 259/2014)²¹ tuvo que resolver sobre la validez de la siguiente cláusula-tipo incorporada por el empresario en los contratos de trabajo:

“Ambas partes convienen expresamente que cualquier tipo de comunicación relativa a este contrato, a la relación laboral o al puesto de trabajo, podrá ser enviada al trabajador vía SMS o vía correo electrónico, mediante mensaje de texto o documento adjunto al mismo, sin menoscabo del cumplimiento por parte de la empresa de los requisitos formales exigidos por la normativa laboral vigente, y según los datos facilitados por el trabajador a efectos de contacto. Cualquier cambio o incidencia con respecto a los mismos, deberá ser comunicada a la empresa de forma fehaciente y a la mayor brevedad posible”²².

El razonamiento del Tribunal Supremo para resolver el problema se construye sobre dos fundamentos bien claros:

1.º El número de teléfono móvil y la dirección de correo electrónico son datos personales que no resultan necesarios para el cumplimiento del contrato, por lo que la licitud de su tratamiento no puede hallarse en la regla del art. 6.1.b) RGPD. Que no resultan ni necesarios ni imprescindibles lo muestra claramente la circunstancia de que “la relación laboral pueda desenvolverse –lo ha veni-

²¹ RJ 2015, 4353.

²² AH 4.º

do haciendo hasta las recientes fechas en que tales avances tecnológicos eran inexistentes— sin tales instrumentos, evidencia que no puedan considerarse incluidos en aquella salvedad general” del art. 6.1.b) RGPD (FJ 3).

- 2.º Al no resultar necesarios para el cumplimiento del contrato la licitud de su tratamiento requerirá el consentimiento del trabajador: el “Tribunal en absoluto niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos” (FJ 3).

La cuestión queda así desplazada a la determinación de las características que debe tener la prestación del consentimiento del trabajador para ser considerada válida, para que se estime que se está ante una “manifestación de voluntad libre, específica, informada e inequívoca” del interesado (art. 4.11 RGPD). El Tribunal Supremo, siguiendo los criterios restrictivos de la normativa de protección de datos, no “niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos”, pero se opone a que “en el contrato de trabajo se haga constar —como específica cláusula/tipo— que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las circunstancias —se trata del momento de acceso a un bien escaso como es el empleo— bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario”. La conclusión es

clara: la falta de garantías para la prestación del consentimiento lleva a considerar “que tal cláusula es nula por atentar contra un derecho fundamental, y que debe excluirse de los contratos de trabajo” (FJ 3).

También sobre una cláusula tipo inserta en los contratos de trabajo que, indirectamente, implica la obligación del trabajador de comunicar su número de teléfono móvil y dirección de correo electrónico trata la SAN de 6 de febrero de 2019 (rec. 318/2018)²³. Indirectamente, porque a lo que se obligaba al trabajador, repartidor de comida a domicilio, era a aportar su propio teléfono móvil en el que debía descargarse la aplicación informática de la empresa facilitada a través de su dirección de correo electrónico. De este modo se pretendía tenerlo geolocalizado durante su jornada laboral²⁴. La sentencia de la Audien-

²³ AS 2019, 905.

²⁴ El texto de la cláusula era el siguiente: “Para el desarrollo de las funciones propias del puesto de trabajo, concretamente en la realización de las funciones de reparto de productos, objeto del presente contrato, el trabajador deberá aportar un teléfono móvil de su propiedad con conexión a internet (Smartphone) que permita la instalación y correcto funcionamiento de la aplicación (app) creada por Telepizpa a dichos efectos.

El teléfono móvil y aplicación mencionados deberán utilizarse durante la totalidad de la jornada laboral del trabajador a efectos de que tanto la empresa como sus clientes puedan realizar un seguimiento en tiempo real y mediante geolocalización, de la ubicación de los pedidos que se realizan.

Será responsabilidad del trabajador acudir al centro de trabajo con el citado dispositivo en plenas condiciones de utilización (batería cargada, tarifa de datos disponible, etc.) y obligación suya desconectarse de la aplicación (app) una vez finalizada su jornada laboral.

La aportación de teléfono móvil por parte del trabajador deberá realizarse en los términos y resto de condiciones de utilización que en cada momento consten en la normativa interna de la empresa y, en caso de incumplimiento de la misma, será de aplicación el régimen disciplinario previsto en el convenio colectivo aplicable.

La negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo al amparo de lo previsto en el artículo 49.1.b) del Texto Refundido de la Ley del Estatuto de los Trabajadores.

Concretamente el trabajador, tendrá un plazo de diez días para repararlo y ponerlo de nuevo en funcionamiento al undécimo día. A partir del momento de la carencia del teléfono

cia Nacional no entra en la valoración del consentimiento del trabajador para el tratamiento de estos datos, por entender que el sistema de geolocalización instalado vulnera de pleno el derecho a la privacidad de los trabajadores²⁵ al establecer un sistema desproporcionado de control²⁶: “la medida implantada, si bien obedece a fines constitucionalmente legítimos en el desarrollo del derecho a la libre empresa como son el control del empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente— de forma que éste pueda conocer en todo momento la ubicación de su pedido, dotando a la empresa de capacidad para proporcionar servicios que se afirma ya ofrecen otras empresas del sector—, no supera a juicio de la Sala el necesario juicio de proporcionalidad”. Esa finalidad legítima “se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados como pudieran ser la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos que no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema” (FJ 6). Pese a que no sea objeto de pronunciamiento en la sentencia, de ella puede deducirse que el consentimiento del trabajador en el momento

de la celebración del contrato resulta irrelevante si el tratamiento es desproporcionado. Se trataría de una específica aplicación del art. 3.1.c) ET: cláusula contractual menos favorable o contraria a disposición legal.

Dentro del segundo grupo, prestación de consentimiento para el tratamiento de datos personales del trabajador que sí están implicados en el objeto del contrato, la STS de 10 de abril de 2019 (rec. 227/2017)²⁷ analiza la validez de una cláusula tipo contenida en los contratos que una empresa del sector de *contact center*, antiguo telemarketing, celebra con sus trabajadores²⁸: “El trabajador consiente expresamente, conforme a la LO 1/1982, de 5 de mayo, RD 1720/2007 de Protección de Datos de carácter personal y Ley Orgánica 3/1985 de 29 de mayo, a la cesión de su imagen, tomada mediante cámara web o cualquier otro medio, siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato y los requerimientos del contrato mercantil del cliente”. La empresa, con unos seis mil trabajadores en plantilla, presta servicios que incluyen la realización de videollamadas. En el momento de la reclamación tenía contratos con dos clientes cuyo cumplimiento exigía la realización de videollamadas en las que intervenían quince trabajadores. Por otra parte, cuando la empresa utiliza la imagen de sus empleados para realizar actividades promocionales les solicita una autorización específica.

En la instancia la SAN de 15 de junio de 2017 (rec. 137/2017)²⁹ declaró la invalidez de

o bien finalizado el período de diez días sin que el trabajador hubiese aportado nuevamente su propio teléfono, se procederá a suspender el contrato de trabajo del citado empleado por un periodo máximo de dos meses. Finalizado dicho periodo el contrato se dará por definitivamente finalizado. Durante el periodo de suspensión” (HP 4º).

²⁵ Como dice MARTÍNEZ MOYA la sentencia “se refiere a la privacidad, sin mayores precisiones, cuando el derecho fundamental a la protección de datos es de más amplio espectro” (cit., p. 7).

²⁶ Además “para la implantación del sistema de geolocalización por parte del empleador se ha prescindido de proporcionar a los trabajadores de la información a que se refieren los arts. 12 y 13 del Reglamento 679/2016, 5 de la anterior Ley de protección de datos y 11 y 90 de la vigente LO 3/2018” (FJ 6).

²⁷ RJ 2019, 1880.

²⁸ CANO GALÁN, Y.: “Cláusulas contractuales tipo sobre cesión de derechos de imagen de los trabajadores y cumplimiento de la normativa sobre protección de datos de carácter personal”, *Diario La Ley*, 24 de Mayo de 2018 (LA LEY 7684/2019). GARCÍA-PERROTE ESCARTÍN, I.; MECADER UGUINA, J. R.: “Datos personales y cláusulas contractuales: los límites del consentimiento en la doctrina reciente del Tribunal Supremo”, *Revista Española de Derecho del Trabajo*, núm. 223 (2019). ARIAS DOMÍNGUEZ, Á.: “Video-llamadas en trabajos de contact-center y cesión de derechos de imagen”, *Revista de Jurisprudencia Laboral*, núm. 3 (2019).

²⁹ AS 2017, 1528.

esta cláusula contractual. Su razonamiento se alza sobre la idea de que no forma parte de la prestación comprometida por el trabajador el uso de su imagen, por lo que su captación requiere el consentimiento del trabajador que no se puede entender prestado libremente en una cláusula tipo del contrato de trabajo:

- a) La captación y uso de la imagen del trabajador resulta imprescindible para la realización de las videollamadas. Sin embargo esta actividad resulta muy infrecuente en la empresa: sólo participan en ella quince de sus seis mil trabajadores.
- b) Por tanto se puede trabajar en esta empresa sin necesidad de que se produzca la captación y uso de la imagen el trabajador, de modo que “no es absolutamente imprescindible para el cumplimiento del objeto del contrato, puesto que se utiliza [la videollamada], al menos hasta ahora, de manera absolutamente excepcional”.
- c) La captación, uso y cesión de la imagen del trabajador por el empresario, al no formar parte del objeto del contrato, requiere el consentimiento expreso del trabajador. Un consentimiento que debe ser específico y distinto del genérico constitutivo del contrato.
- d) Ese consentimiento no puede expresarse en la cláusula tipo incluida en el contrato de trabajo puesto que la situación de inferioridad en que se encuentra el trabajador en el momento de celebrar el contrato impide que se pueda hablar de un consentimiento libre de acuerdo con la STS de 21 de septiembre de 2015.
- e) El momento idóneo para manifestar el consentimiento del trabajador surgirá “cuando la empresa destine a sus trabajadores a la realización de servicios de video llamada, porque lo requiera así el contrato mercantil con el clien-

te, deberá solicitar, en ese momento, el consentimiento del trabajador, que deberá ajustarse de manera precisa y clara a los requerimientos de cada contrato, sin que sea admisible la utilización de cláusulas tipo de contenido genérico, que no vayan asociadas a servicios concretos, requeridos por contratos específicos, por cuanto dicha generalización deja sin contenido real el derecho a la propia imagen de los trabajadores, que queda anulado en la práctica, aunque se diera consentimiento genérico al formalizar el contrato”.

El Tribunal Supremo, sin embargo, ha declarado la validez de la cláusula contractual. Con carácter general parte de que la imagen³⁰ constituye un dato personal cuya captación y tratamiento requiere el consentimiento del interesado, salvo que sea necesario para la ejecución de un contrato del que se es parte (6.1.b RGPD). Descendiendo al caso concreto planteado en esta empresa, considera que la participación en videollamadas forma parte del oficio del trabajador, de su prestación laboral, por lo que se trata de realizar “funciones propias del objeto del contrato celebrado, aunque no sean las habituales” (FJ 2)³¹. A ello no obsta la reducida incidencia y frecuencia con se requieren los servicios de videollamada en la empresa, sólo con dos clientes y por quince trabajadores entre los seis mil de la empresa, “porque lo importante no es el mayor o menor uso que se haga de esa función, sino que el consentimiento está implícito en el contrato por su objeto y además

³⁰ Véase CRISTÓBAL RONCERO, R.: “Protección del derecho a la propia imagen en el trabajo”, *Nueva Revista Española de Derecho del Trabajo*, núm. 199 (2017), pp. 75 a 95.

³¹ El “objeto del contrato y su ejecución es la realización de labores de telemarketing incluso con video-llamadas, lo que es hasta cierto punto lógico porque, dados los avances tecnológicos existentes, la capacidad de inspirar confianza y de convencer es mayor cuando vemos la cara de nuestro interlocutor y deseamos la idea de que se habla con una máquina o con un desconocido. En este sentido se puede señalar que la información sobre una mercancía y su venta resultan más fáciles cuando el comprador ve el producto y al vendedor, como en las tiendas tradicionales” (FJ 2).

que se ha explicitado en él por el trabajador, quien en todo momento puede revocarlo (art. 7 del Reglamento), o negarse a realizar tareas en condiciones que escapen al contenido propio de su contrato, sin perjuicio de las consecuencias que ello pueda tener” (FJ 2).

Una vez afirmado que la participación en videollamadas forma parte de la prestación del trabajador las consecuencias se derivan necesariamente: a) no será necesario el consentimiento del trabajador para su tratamiento, sino que estaremos ante la excepción del art. 6.1.b) RGPD; y b) la cláusula contractual en cuestión es válida y en cuanto expresa un consentimiento del trabajador innecesario, pues va dirigido a autorizar un tratamiento de datos requerido para el cumplimiento del contrato, cumple una finalidad meramente informativa. Así puede leerse en su fundamento jurídico segundo: “si se trata de la realización de funciones propias del objeto del contrato celebrado, aunque no sean las habituales, es lo cierto que la cláusula controvertida se limita a advertir al nuevo contratado de la posibilidad de tener que realizar una de las funciones propias del contrato que suscribe y, a la par que el mismo queda advertido de ello, presta, expresamente, su consentimiento a la cesión de su imagen, pero con una salvaguarda: “siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato”, esto es que la cesión de la imagen, el dato, venga condicionada a que su fin sea cumplir con el objeto del contrato”. Por tanto la cláusula controvertida “no es abusiva, sino, más bien, informativa y a la par receptora de un consentimiento expreso que no era preciso requerir”, de acuerdo con la normativa de protección de datos conforme a la cual “el consentimiento no es necesario prestarlo hoy día, ni lo era entonces, cuando los datos, la imagen, se ceden en el marco del cumplimiento de un contrato de trabajo cuyo objeto lo requiere. Por ello, la cláusula controvertida no se puede considerar abusiva, ni calificar de nula, porque es lícita, dado que es manifestación de un consentimiento expreso que el trabajador da a la cesión de su imagen,

cuando la actividad propia del telemarketing, la del convenio colectivo, la desarrolle por video-llamada y que está implícito en el objeto del contrato” (FJ 2).

El Tribunal Supremo cierra su argumentación distinguiendo el supuesto examinado de los que fueron objeto de decisión en la STC 99/1994, de 11 de abril y en la ya citada STS de 21 de septiembre de 2015. En el archiconocido caso de la STC 99/1994 sobre el deshuesador de jamones, la cesión de la imagen del trabajador no formaba parte de las tareas contratadas lo que sí sucede en el supuesto ahora resuelto: por tanto en el caso de la empresa de *contact center* la restricción de los derechos a la propia imagen y a la protección de datos personales “viene impuesta por la naturaleza de las tareas contratadas” (FJ 2). Por otra parte, la distinción con el supuesto de la STS de 21 de septiembre de 2015 es obvia: en ella se enjuició una cláusula contractual en virtud de la cual el trabajador aceptaba el tratamiento de datos innecesarios para el cumplimiento del contrato, mientras que en ésta la cláusula enjuiciada “se limita a expresar cual puede ser una de las labores a realizar y la aceptación de ese deber” (FJ 2).

* * * * *

No son infrecuentes los pactos, individuales o colectivos³², en virtud de los cuales el empresario asume la obligación de concertar algún tipo de seguro en favor del trabajador, por

³² Un par de ejemplos. *Convenio colectivo estatal del sector de desinfección, desinsectación y desratización* (BO de 10 de abril de 2018). Artículo 32. Seguro colectivo de accidentes. Las empresas establecerán un seguro colectivo de accidentes para todos/as los/as trabajadores/as que garanticen a los mismos la percepción de 16.500- euros, en caso de que como consecuencia del accidente el/la trabajador/a quede en situación de incapacidad permanente absoluta, o de 23.100- euros si como consecuencia del accidente se produjera el fallecimiento, cantidad que percibirán sus beneficiados. *Convenio colectivo de centros de asistencia y educación infantil* (BOE de 26 de julio de 2019). Artículo 75. Responsabilidad civil y accidentes. Todos los Centros deberán contratar pólizas de seguros que garanticen la cobertura de accidentes y responsabilidad civil de todo el personal afectado por este Convenio. Deberán estar en vigor durante el período correspondiente, pudiendo prorrogarse o modificarse a petición de las organizaciones firmantes.

lo que también en el momento de la contratación habrá que proceder a la recogida y tratamiento de sus datos personales a tal efecto. Tratándose de una condición más beneficiosa individual o de una obligación impuesta por el convenio colectivo la licitud del tratamiento derivaría del art. 6.1.b) RGPD (tratamiento necesario para la ejecución de un contrato del que se es parte), pues tanto el contrato como el convenio colectivo son fuente de la relación laboral [art. 3.1.b) y c) ET]³³.

Como señala la Guía de la Agencia Española de Protección de Datos (en adelante, AEPD) *La protección de datos en las relaciones laborales en estos casos*³⁴ el empresario puede realizar uno de estos dos tratamientos de datos: la comunicación a la aseguradora de los datos de contacto del trabajador para que ésta recabe los datos necesarios a efectos de formalizar el seguro correspondiente o la recogida y comunicación a la aseguradora de todos los datos necesarios. El tratamiento de datos en ambos casos, también según la Guía citada, estaría legitimado por el consentimiento del trabajador o por el propio contrato de trabajo. La Guía señala que “desde el punto de vista de un tratamiento absolutamente respetuoso con el derecho fundamental lo más adecuado puede consistir en, previa información a los trabajadores, ceder a la aseguradora, o a la gestora del plan de pensiones, únicamente los datos de los asegurados o partícipes del plan de pensiones, dejando en sus manos el desarrollo de ulteriores gestiones”³⁵.

La AEPD ha tenido ocasión de examinar en su Resolución E/02259/2015 la cesión de datos del trabajador por parte del empresario a la empresa depositaria de un plan de pensiones. Este plan se configura como premio de fidelización para los trabajadores de cierta antigüe-

dad, es adicional a otros planes de pensiones y ahorro con los que ya contaba la empresa y forma parte de su club de fidelización. La adhesión de los trabajadores al plan se produce de modo automático al alcanzar la antigüedad requerida, de acuerdo con lo previsto en el art. 28.2 del Reglamento de Planes y Fondos de Pensiones (incorporación directa del trabajador al plan en virtud de acuerdo adoptado por la empresa con los representantes de los trabajadores, con información al trabajador y derecho de éste a oponerse a la incorporación)³⁶.

³⁶ RD 304/2004, de 20 de febrero. Artículo 28. Adhesión de partícipes en planes de empleo.

1. Efectuada la comunicación de la admisión del plan en el fondo prevista en el artículo anterior, podrá hacerse efectiva la incorporación al plan de partícipes, y la comisión promotora del plan de empleo deberá instar la constitución de la pertinente comisión de control del plan en un plazo no superior a 12 meses desde la formalización del plan. En tanto no se constituya la comisión de control, las funciones atribuidas a ésta por este Reglamento corresponderán a la comisión promotora.

2. Cuando en el convenio colectivo se haya establecido la incorporación de los trabajadores directamente al plan de pensiones, se entenderán adheridos a éste, salvo que, en el plazo acordado a tal efecto, declaren expresamente por escrito a la comisión promotora o de control del plan que desean no ser incorporados al plan. Lo anterior se entenderá sin perjuicio de que, en su caso, el convenio condicione las obligaciones de la empresa con los trabajadores a su incorporación al plan de pensiones.

Asimismo, en virtud de acuerdo adoptado por la empresa con los representantes de los trabajadores en ésta, la comisión promotora, una vez formalizado el plan de pensiones del sistema de empleo, podrá efectuar directamente la incorporación al plan de los partícipes y, en su caso, de los beneficiarios, debiendo señalarse un plazo para que los que no deseen incorporarse al plan se lo comuniquen por escrito. También será admisible la suscripción de documentos individuales o colectivos de adhesión al plan del sistema de empleo en virtud de delegación expresa otorgada por los partícipes.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio de que, en su caso, el convenio colectivo o disposición equivalente que establezca los compromisos por pensiones condicione la obligación de la empresa a su instrumentación a través de un plan del sistema de empleo, o de las acciones y derechos que corresponda ejercitar en caso de discrepancia o información inadecuada sobre los procesos de incorporación al plan.

3. El trabajador que reúna las condiciones para acceder al plan podrá ejercitar su derecho de incorporación en cualquier momento y en tanto no se haya extinguido la relación laboral con el promotor, sin perjuicio del régimen de aportaciones y prestaciones aplicable en cada caso.

³³ Los datos necesarios para el mantenimiento y cumplimiento del contrato de trabajo incluyen “no sólo las obligaciones derivadas del contrato de trabajo, sino también las impuestas por la ley y, de manera más problemática, las que puedan derivar de otras normas laborales, como el convenio colectivo” (DENTADO BONETE; MUÑOZ RUIZ: cit., p. 105).

³⁴ Página 16.

³⁵ Página 17.

En el caso contemplado, la empresa informó a los trabajadores a través de diversas acciones internas (eventos en tienda, reparto de información y comunicación en distintos soportes, noticias en la intranet corporativa, carteles informativos, etc.) y disponía de una plataforma *online* para que los empleados pudieran comprobar los requisitos de acceso al programa, recabar información y cursar baja en caso de no estar interesados. La AEPD estimó que existía un consentimiento tácito del trabajador para el tratamiento de sus datos por dos razones: el trabajador solo formuló la denuncia un año después de la constitución del plan y este plan resultaba complementario de otros de los que ya era beneficiario. También estimó que el empresario había cumplido con su deber de informar a través de las diferentes acciones antes descritas. Por todo ello la AEPD afirmó que la cesión de datos a la entidad depositaria del plan había sido legítima según el art. 11.2.c) LOPD-1999³⁷. Téngase en cuenta que con la normativa vigente no resulta admisible el consentimiento tácito³⁸, por lo que en cuanto en estos casos se trate de una obligación derivada de las reglas del contrato (legales, convencionales o contractuales) será el cumplimiento de éste la fuente de legitimación del tratamiento.

2.2. Tratamiento de datos necesario para el cumplimiento de obligaciones legales del empresario

Con la celebración del contrato de trabajo surgen varias obligaciones del empresario que van a requerir el tratamiento de datos

Teniendo en cuenta lo previsto en el artículo 25.2, párrafo segundo, en los casos en que se prevea la incorporación al plan de trabajadores que hubieran extinguido su relación laboral con el promotor, las especificaciones precisarán las condiciones para su incorporación y el régimen de aportaciones y prestaciones aplicable.

³⁷ No será necesario el consentimiento del interesado "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros".

³⁸ Preámbulo de la LOPDGDD, apartado V.

personales del trabajador: la comunicación del contrato a la oficina pública de empleo (art. 8.3 ET), la entrega de la copia básica del contrato a los representantes de los trabajadores (art. 8.4 ET) y el alta del trabajador en la Seguridad Social (arts. 16, 139 y 140 LGSS). En todos estos casos se va a producir lo que la LOPD-1999 definía como "cesión o comunicación de datos" [art. 3.j)], es decir, una "revelación de datos realizada a una persona distinta del interesado", un tercero (administración pública, representantes de los trabajadores). La cesión o comunicación de datos exigía, como regla general, el previo consentimiento del interesado junto con la legitimidad del fin para el que se producía la cesión (art. 11.1). Esta regla general contemplaba varias excepciones entre las cuales se encontraban dos que resultaban particularmente aplicables en la relación laboral: la autorización de la ley [art. 11.2.a)] y la "libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros" [art. 11.2.c)]. Sin embargo ni el RGPD ni la LOPDGDD establecen un régimen específico para la cesión o comunicación de datos, por lo que resulta aplicable el régimen general del tratamiento³⁹. En efecto, el art. 4.2) RGPD incluye la comunicación entre las operaciones integradas en la noción de tratamiento y el art. 4.9) RGPD define al "destinatario" como la persona, autoridad pública, servicio u otro organismo al que se comuniquen datos personales. Será por tanto el criterio del art.6.1.c) RGPD, tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento⁴⁰, el fundamento de este tipo de tratamiento de datos.

De acuerdo con los arts. 8.4 y 64.4 ET el empresario debe entregar a la representa-

³⁹ MESSÍA DE LA CERDA BALLESTEROS, J. A.: "La evolución del concepto de cesión o comunicación de datos personales", *Actualidad Civil*, núm. 10 (2017), p. 8 (citado según versión digital La Ley 14126/2017).

⁴⁰ Art. 8.1 LOPDGDD.

ción de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito. El contrato contiene datos personales del trabajador de los que debe excluirse en la copia básica el número del documento nacional de identidad, el número de identidad del extranjero, el domicilio, el estado civil y cualquier otro que pudiera afectar a la intimidad personal. El art. 8.4 ET impone al empresario la obligación de entregar a los representantes de los trabajadores una copia básica del contrato, por lo que la entrega de cualquier copia que no fuera “básica” no podría estar fundada en el art. 6.1.c) RGPD. Conforme al art. 5.1.b) RGPD estos datos no podrán ser tratados ulteriormente de manera incompatible con el fin para el que son recogidos: comprobar la adecuación del contenido del contrato a la legalidad vigente (art. 8.4 ET).

El salario ha sido el dato personal contenido en el contrato de trabajo que ha generado una mayor conflictividad en relación con el cumplimiento de la obligación impuesta por el art. 8.4 ET. Una litigiosidad, por otra parte, tangencial al derecho a la protección de datos personales como se explica a continuación.

- a) A raíz de la promulgación de la Ley de 2/1991, de 7 de enero, precedente del vigente art. 8.4 ET, se discutió si el salario es un dato personal que afecta a la intimidad del trabajador. La consecuencia de la respuesta a esa cuestión era importantísima: si es dato que afecta a la intimidad del trabajador debe excluirse de la copia básica que se entrega a la representación de los trabajadores. La cuestión fue resuelta por la STC 142/1993, de 22 de abril en el sentido de que el salario no es dato relativo a la intimidad del trabajador. Por tanto será el derecho a la protección de datos el único que se vea afectado con su tratamiento por el empresario en estos casos pues, como es bien sabido, se trata de derechos autónomos: mientras el derecho a la intimidad se refiere a datos íntimos el

de protección de datos afecta a cualesquiera datos personales⁴¹.

- b) El otro factor de litigiosidad no afecta tanto al derecho a la protección de datos como al ámbito del derecho de información de los representantes de los trabajadores. Se trata de la práctica de configurar el contenido de determinadas cláusulas contractuales por remisión al convenio colectivo aplicable (“según convenio”). Surge entonces el conflicto entre el empresario que entiende cumplida su obligación con la entrega de la “copia” básica en la que tal cual se trasladan las cláusulas “según convenio”, pues una copia es “una reproducción literal” de un escrito de modo que no puede aparecer en la copia lo que no consta en el original, y los representantes de los trabajadores que no se conforman con la entrega de la “copia”, sino que exigen la determinación precisa de la correspondiente condición contractual. Como puede apreciarse es cuestión que no afecta al derecho a la protección de datos personales, pues éstos han de comunicarse a los representantes de los trabajadores tanto si hay determinación específica o como si se efectúa por remisión al convenio colectivo aplicable, sino al ámbito del derecho de información de estos representantes. La STS de 24 de marzo de 1998 (rec. 2714/1997)⁴² declaró que el empresario no sólo no está obligado a comunicar datos distintos de los que figuran en el texto original, sino que si así lo hiciera estaría incumpliendo la obligación que el art. 8.4 ET le impone (FJ 3). En el mismo sentido resuelve la reciente SAN 118/2019, de 18 de octubre de 2019⁴³: “si se solicita que se declare el derecho a que la copia básica de los contratos que entregue la empresa figuren determinados datos y, en la medida que

⁴¹ TRONCOSO REIGADA: *cit.*, p. 5.

⁴² RJ 1998, 3009.

⁴³ JUR 2019, 302523.

tales datos no figuran en los contratos originales, no es posible incluir tales datos formando parte de la copia, sin que el mandato legal amplíe la obligación de suministrar a los representantes legales de los trabajadores datos que no figuran en el contrato original” (FJ 2).

3. RECOGIDA Y TRATAMIENTO DE DATOS DURANTE EL CUMPLIMIENTO DEL CONTRATO DE TRABAJO

El derecho a la protección de datos, más allá de los supuestos de recogida y tratamiento de datos de los trabajadores, puede condicionar aspectos importantes del desarrollo de la relación laboral. Un buen ejemplo es la llamada política de “escritorios limpios” adoptada por empresas que tienen acceso y tratan datos personales de sus clientes. Esta política de “escritorios limpios” va dirigida a garantizar la seguridad de los datos de sus clientes evitando, particularmente, que los trabajadores de la empresa con acceso a los datos hagan un uso ilícito de los mismos⁴⁴ y para ello se prohíbe la introducción en los lugares de trabajo de efectos que podrían utilizarse para apropiarse de esos datos (bolsos, mochilas, abrigos, memorias usb, teléfonos móviles, memorias externas, software de intercambio de ficheros, software de mensajería instantánea, PDAs, cámaras digitales, papel y bolígrafos)⁴⁵, de modo que el escritorio esté “limpio” de todos esos objetos, sobre todo limpios de papel, de instrumentos de escritura y de aparatos electrónicos que permitan la captación y almacenamiento de datos personales.

Son decisiones empresariales que entran dentro del ámbito de ejercicio del poder empresarial para dirigir y organizar el trabajo

pero que, en algún supuesto, pueden entrar en conflicto con otros derechos y bienes jurídicamente protegidos como muestra la existencia de algunos litigios. En la SAN de 15 de noviembre de 2018 (rec. 187/2018)⁴⁶ se plantea la compatibilidad de estas políticas empresariales con los derechos de los representantes de los trabajadores a difundir información [arts. 8.1.b) y c) LOLS y 68.d) ET], concretamente si la política de “escritorios limpios” podría excluir la distribución de comunicados sindicales en papel y la utilización de teléfonos móviles. El tribunal resuelve la cuestión aplicando el principio de proporcionalidad, llegando a soluciones distintas para cada uno de estos dos problemas.

En relación con la distribución de información sindical en papel el tribunal entiende que el derecho a difundir información de los representantes de los trabajadores sólo podría verse limitado por las medidas de seguridad que la empresa puede legítimamente imponer si fueran idóneas, razonables y proporcionadas al fin pretendido. Para ello la empresa debería haber acreditado que “la introducción de papel escrito en las plataformas constituye un riesgo patente y actual, aunque no se permita a los trabajadores introducir medios para escribir en él, para la seguridad de los datos personales de sus clientes y usuarios” (FJ 4). Al no haberlo hecho “la prohibición de introducir papel escrito en las plataformas, teniendo en cuenta, además, que no se permite ningún medio para escribir en dichos papeles, si es que pudiera escribirse algo en ellos, es absolutamente inidónea, irrazonable y desproporcionada” (FJ 4). Tampoco cabe, a juicio de la sala, imponer unilateralmente la distribución de la información sindical por medios digitales salvo “que se hubiera acreditado, que no es el caso, que la introducción de comunicados en papel constituyera una amenaza exorbitante para la seguridad de los datos” (FJ 4). La conclusión es clara: los representantes de los trabajadores tienen derecho a distribuir en

⁴⁴ El objetivo básico de esta política, dice la SAN de 15 de noviembre de 2018 (rec. 187/2018), es “asegurar que no se filtre información sobre datos reservados” de los “clientes y usuarios” (FJ 4). Véase también, sobre supuesto idéntico, la SAN de 3 de mayo de 2019 (rec. 60/2019; AS 2019, 1630).

⁴⁵ SAN de 15 de noviembre de 2018 (rec. 187/2018).

⁴⁶ AS 2019, 164.

los puestos de trabajo “información sindical en papel, siempre que se notifique a la empresa y no se disturbe la actividad normal del trabajo” (FJ 4).

Distinta es la respuesta del tribunal a la pretensión del sindicato reclamante de permitir el uso de teléfonos móviles “porque su prohibición les impedía comunicarse eficientemente con sus sindicatos y sus representantes” (HP 7), petición a la que la empresa había respondido habilitando teléfonos móviles en el puesto de trabajo que sólo se podrían utilizar para “cuestiones sindicales” (HP 7). La solución del tribunal se construye sobre dos argumentos: a) el empresario puede impedir el uso de teléfonos móviles en la empresa por razones de seguridad; y b) la incomunicación telefónica de los representantes podría impedir el desarrollo de sus funciones sindicales. En el caso concurre la primera circunstancia, es razonable prohibir el uso de teléfonos móviles dada su idoneidad para fotografiar datos relevantes y la imposibilidad de su control absoluto, pero no la segunda, puesto que la empresa facilita teléfonos móviles en caso de necesidad. Por tanto, como la empresa había puesto a disposición de los representantes de los trabajadores teléfonos suficientes para que puedan recibir llamadas del exterior y comunicarse con sus sindicatos y asesores se desestima la pretensión “puesto que pueden ejercitar, sin impedimentos reales, su función sindical dentro de la empresa, quien está legitimada para no autorizar móviles en el centro de trabajo por unos motivos de seguridad, [...] razonables” (FJ 5).

3.1. Empresa, clientes y datos de los trabajadores

Las relaciones de una empresa con sus clientes generan situaciones, de modo destacado en el sector servicios, en las que puede haber interés en que los clientes tengan acceso a datos personales de sus trabajadores por muy variadas razones: desde la protección de la seguridad de personas y cosas hasta la me-

jora de la calidad empresarial pasando por la asunción de responsabilidades derivadas del negocio. Por otra parte el tipo de datos sobre los que puede recaer este interés son también variados: desde la simple identificación de los trabajadores hasta los que forman parte del contenido de la relación laboral.

Los trabajadores son la imagen de la empresa, quienes prestan los servicios correspondientes al cliente que tiene en ellos su punto de referencia y conexión con la empresa. No es de extrañar, por tanto, que el art. 19 LOPDGD declare que, salvo prueba en contrario, se presumirá amparado en el art. 6.1.f) RGPD (satisfacción de intereses legítimos) el tratamiento de los datos de contacto y los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica, siempre que el tratamiento se refiera a los datos necesarios para su localización profesional y su finalidad sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios⁴⁷.

Un ejemplo de la problemática a que puede dar lugar el tratamiento de datos personales de los trabajadores con la finalidad de identificarlos ante los clientes puede verse en la STS de 18 de diciembre de 2006 (rec. 112/2005)⁴⁸. El conflicto se plantea en unos grades almacenes en los que los trabajadores exhiben tarjetas identificativas y se hace constar en los recibos de compra de los clientes el nombre y apellidos del vendedor, precedido de las abreviaturas “Sr.” o “Srta”. Antes de implantar este nuevo sistema, que se ha hecho sin recabar el consentimiento expreso de los tra-

⁴⁷ Precedente de esta norma es el art. 2.2 del Reglamento de desarrollo de la LOPD-1999 (Real Decreto 1720/2007, de 21 de diciembre): “este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales”.

⁴⁸ RJ 2007, 750.

bajadores afectados, en los *tickets* de compra sólo aparecía un número de identificación del vendedor. Se impugnó la decisión empresarial por entender que constituía una lesión del derecho a la intimidad de los trabajadores afectados, al no estar expresamente autorizada por la ley ni existir un interés empresarial o de tercero que la justificara ni ser necesaria o imprescindible.

El Tribunal Supremo no consideró que hubiera lesión del derecho a la intimidad de los trabajadores, pues los datos tratados carecían de naturaleza íntima y eran los usados “en todo tipo de relaciones humanas en contacto con el público” (las abreviaturas Sr. o Srta. se consideran mera fórmula de cortesía aplicable con independencia del estado civil de la mujer). Además se trata de una medida que atiende a fines legítimos en interés tanto del empresario como del trabajador. Si por una parte busca mejorar la atención al cliente, por otra “sirve a la fundamental tarea de dignificar la persona, evitando su cosificación, individualizándolo del resto de sus compañeros, dotándole de la dignidad que le corresponde al evitar designarlo con una clave numérica como un mero factor de producción” (FJ 2). Apareciendo así como una “medida idónea, necesaria y proporcionada” (FJ 2).

El derecho a la protección de datos personales no aparece mencionado específicamente en la argumentación de la sentencia pero se utilizan razonamientos que muy bien se hubieran podido aplicar para excluir su infracción. Frente a la hipótesis de que se tratara de datos personales tratados sin consentimiento del trabajador se alza la necesidad del tratamiento para el cumplimiento de contratos de los que es parte: “las tareas encomendadas al trabajador implicaban la restricción de su derecho a permanecer en el anonimato de tal suerte que pudiera entenderse que era la propia voluntad del trabajador —expresada al celebrar el contrato— la que legitimaba la misma, pues es claro que existen actividades que traen consigo, con una relación de conexión necesaria, una restricción en tal derecho

por su propia naturaleza, como son las actividades en contacto con el público o accesibles a él”. También se desestima la alegación de que el posible uso del nombre y apellidos del trabajador coordinado “con los que son objeto de divulgación general, como el domicilio y el número de teléfono (por ejemplo a través de la guía telefónica)” pudiera ofrecer “una imagen casi completa de los aspectos vinculados a su intimidad”, porque “si el cliente estuviese interesado en conocer estos otros aspectos, también podría realizar tal coordinación partiendo de los datos consignados en la placa de identificación”.

Sí hay referencia expresa a la normativa de protección de datos en otro caso, resuelto por la STSJ Madrid de 30 de junio de 2008 (rec. 2351/2008)⁴⁹, en el que se discutía la licitud de la comunicación del nombre, apellidos y número de documento nacional de identidad del trabajador por parte de su empresario a un cliente. La empresa había concertado un contrato de prestación de servicios con una compañía de seguros (empresa cliente) en virtud del cual se encargaría de la atención a sus asegurados, para lo cual los trabajadores de la empresa de servicios debían acceder a las bases de datos de la compañía de seguros. A tal efecto la empresa de servicios comunicó a la compañía de seguros el nombre, apellidos y documento nacional de identidad del trabajador, discutiéndose en el caso si se trataba de una cesión ilícita de datos personales al efectuarse sin consentimiento del trabajador. La sentencia del TSJ de Madrid entendió que el consentimiento del trabajador era innecesario en este caso pues el tratamiento de datos tenía su fundamento en el cumplimiento del contrato de trabajo (art. 6.2 LOPD-1999), “pues en definitiva se trata del desarrollo de una campaña de soporte de telemarketing, consistente en prestar asistencia telefónica a los clientes de la empresa principal [...] y para ello es necesario la aportación por la contratista de unos mínimos datos personales del trabajador

⁴⁹ AS 2008, 2186.

adscrito a tales cometidos, a fin de poder entrar en contacto con las bases de datos de sus clientes, lo que se revela así en indispensable, tanto para el mantenimiento de dicha vinculación, como para el cumplimiento del contrato de trabajo, por lo que ha de concluirse que en tal supuesto no es necesario el previo consentimiento del trabajador afectado” (FJ 2).

Sobre la comunicación del número del documento nacional de identidad de los trabajadores tiene interés la STS (CA) de 25 abril de 2016 (rec. 49/2014)⁵⁰ que declaró la nulidad de la previsión contenida en la Orden INT/318/2011, de 1 de febrero sobre Personal de Seguridad Privada. Según esta disposición debía constar en la tarjeta de identidad profesional del personal “el número del Documento Nacional de Identidad o del Número de Identificación de Extranjero, con todos sus caracteres alfanuméricos”. Para el Tribunal Supremo “la necesidad de identificación del personal de seguridad privada ante los cuerpos de seguridad y ante los ciudadanos afectados que por razones del servicio así lo soliciten [...] no exige la constancia en la tarjeta de identidad profesional del número de DNI o del Número de Identificación de Extranjero, pues como razona la sentencia [...] recurrida [...], la identificación de los vigilantes de seguridad resulta del conjunto de datos expresados en la tarjeta de identidad profesional (entre ellos la fotografía, el nombre y apellidos, las habilitaciones para las que el documento autoriza a su titular y el número y fecha de cada habilitación), y puede reforzarse con facilidad con otro número o registro que no sea coincidente con el número del DNI, por lo que es acertada la conclusión de la Sala de instancia de que no resulta indispensable para la identificación que el número de la tarjeta coincida con el número del DNI” (FJ 4)⁵¹.

La comunicación de la fotografía de los trabajadores al cliente es un supuesto sobre el que se pronuncia el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo sobre Protección de Datos del Artículo 29. La licitud del tratamiento de este dato dependerá del carácter no excesivo de su recogida y tratamiento en función del servicio prestado al cliente. Por lo que si el tratamiento no es proporcionado carecerá de fundamento, sin que se pueda basar en el consentimiento del trabajador pues éstos “no están en condiciones, habida cuenta del desequilibrio de poder, de dar su libre consentimiento al tratamiento de sus datos personales”. El mismo dictamen pone el ejemplo de la empresa de mensajería que, amparándose en su interés legítimo, comunica a sus clientes un enlace al nombre y ubicación de los repartidores así como una foto de su pasaporte que permitiría al cliente comprobar si el repartidor es la persona correcta. El dictamen afirma que “no es necesario facilitar el nombre y foto del repartidor a los clientes” y que “dado que no existe ningún otro motivo legítimo para este tratamiento, la empresa de mensajería no está autorizada a facilitar estos datos personales a los clientes”.

Como puede apreciarse en estos dos últimos supuestos sobre tratamiento del número de documento nacional de identidad y de la fotografía de los trabajadores, la legitimidad del fin con que se recogen estos datos personales y su carácter adecuado, pertinente y limitado en relación con dicho fin [art. 5.1.b) y c) RGPD] serán los elementos que permitan plantear el criterio de licitud del tratamiento (art. 6 RGPD).

* * * * *

Un cliente muy singular es el empresario (empresario principal) que contrata con otro (empresario auxiliar) la realización de obras o servicios correspondientes a su propia actividad empresarial (art. 42 ET). El empresario principal es responsable solidario de las obligaciones de naturaleza salarial y de seguridad social contraídas por los empresarios auxilia-

⁵⁰ RJ 2016, 2026.

⁵¹ Véanse, no obstante, en SAN MARTÍN MAZZUCCONI (*cit.*, pp. 235 y 236) los Informes de la AEPD que consideran adecuada a la normativa de protección de datos la inclusión del número del DNI en tarjetas identificativas de trabajadores.

res durante la realización de las correspondientes obras o servicios (art. 42.2 ET). Se entiende que exista en estos casos un interés legítimo del empresario principal en tener acceso a los datos salariales y de seguridad social de los trabajadores de los empresarios auxiliares frente a los cuales puede ser declarado responsable solidario.

Esta cuestión se planteó en el Informe 0412/2009 de la AEPD⁵², concretamente si la comunicación de los recibos de salario (la “nóminas”) y los documentos de cotización de los trabajadores de una empresa auxiliar al empresario principal resultaría ajustada a la normativa de protección de datos personales. Este Informe concluyó que la comunicación de dichos datos se encontraba amparada por la LOPD-1999: puesto que el empresario principal es responsable solidario de las obligaciones salariales y de seguridad social generadas durante la contrata debería conocer el contenido íntegro de dicha obligación para poder cumplirla. El tratamiento de datos que implica esta comunicación no requeriría el consentimiento del trabajador afectado, al tener por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario. Sin embargo la cuestión puede complicarse pues en algunos casos los documentos de cotización pueden contener datos relativos a la salud del trabajador y la nómina el dato de afiliación sindical que son datos especialmente protegidos (art. 9 RGPD). En relación con los documentos de cotización que contuvieran datos relativos a la salud del trabajador el Informe citado concluyó que su cesión estaría amparada por el art. 7.3 LOPD-1999 (tratamiento de los datos de salud cuando “lo disponga una ley o el afectado consienta expresamente”) en relación con el art. 42.2 ET. Puesto que el Estatuto de los Trabajadores “impone un deber al empresario principal” la comunicación del TC resultaría adecuada a la normativa de protección de datos “pues se haya expresamente prevista en una norma

con rango de Ley. Además el propio Código Civil exige atender íntegramente las obligaciones solidarias por lo que es preciso conocer el contenido de la misma”. En la normativa vigente la comunicación de los documentos de cotización vendría amparada por el art. 9.2.b) RGPD “en relación con el ET art. 42.2 y por el alcance que Código Civil impone a las obligaciones solidarias”⁵³. En relación con las nóminas que contuvieran el dato de la afiliación sindical el Informe citado llegó a la conclusión de que su cesión al empresario principal resultaba lícita. Para ello realizó una interpretación conjunta de los arts. 7.2 (la afiliación sindical es dato que sólo puede ser objeto de tratamiento con el consentimiento del afectado) y 4.2 LOPD-1999 (prohibición de uso de los datos objeto de tratamiento para finalidad incompatible para la que hubieran sido recogidos). A la vista de ambos el Informe señaló que “el tratamiento del dato relativo a la afiliación sindical se efectúa por el empresario, para que de la nómina se detraiga la cuota sindical correspondiente. Dado que la finalidad de dicho tratamiento va ligada al pago de la nómina y que en virtud de la obligación solidaria que impone el artículo 42.2 del Estatuto de los Trabajadores, al contratista principal, para el pago de las deudas salariales correspondientes, podemos concluir que el tratamiento de dicha información es para un fin idéntico del que justifica el tratamiento efectuado por el subcontratista. Por ello, siendo los fines idénticos, podemos entender que la comunicación de dichos datos es conforme con el artículo 7.2 en conexión con el art. 4.2 de la Ley Orgánica 15/1999 y la obligación impuesta por el artículo 42.2 del Estatuto de los Trabajadores”.

* * * * *

Junto a casos, como los anteriores, en que se efectúa una comunicación de datos desde la empresa a los clientes, también hay otros en los que los datos recorren el camino inverso: del cliente a la empresa. No es infrecuente que un empresario (cliente) externalice la gestión de

⁵² Reproducido por el Informe 0223/2009.

⁵³ MERCADER UGUINA: p. 209.

recursos humanos en una empresa especializada que, entre otras cosas, se ocupará de confeccionar las nóminas de sus trabajadores y de las gestiones de seguridad social⁵⁴, produciéndose así un *data outsourcing*⁵⁵. En estos casos el contratista deberá tratar los datos personales de los trabajadores necesarios para la confección de las nóminas, asumiendo la posición de “encargado del tratamiento”, es decir, de persona que trata datos personales por cuenta del responsable del tratamiento (art. 4.8 RGPD) que es el empresario de los trabajadores. La figura del encargado del tratamiento está minuciosamente regulada en el art. 28 RGPD que determina las principales obligaciones derivadas del contrato que vincula al responsable con el encargado del tratamiento (art. 28.3 RGPD). El encargado, que no podrá subcontratar el encargo salvo autorización previa del responsable (art. 28.2 RGPD), debe ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado (art. 28.1 RGPD). A la figura del encargado del tratamiento se refiere el art. 33 LOPDGDD. Conforme a este precepto el acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla con la normativa de protección de datos.

3.2. Poderes empresariales y protección de datos personales

El ejercicio de los poderes empresariales de dirección, control y sanción de los tra-

bajadores va unido muy frecuentemente al tratamiento de datos personales. Puesto que varios estudios de este volumen se dedican al análisis específico de las implicaciones que el derecho a la protección de datos sobre las facultades de control del empresario, aquí sólo se hará mención a la casuística que ha planteado la aplicación en algunas empresas de programas de evaluación del desempeño de sus trabajadores. Estas evaluaciones se plasman en datos personales⁵⁶ cuya recogida y tratamiento por el empresario estaría fundada en el art. 6.1 RGPD. Los problemas surgen cuando esos datos personales salen fuera de la relación anudada entre empresario y trabajador, comunicándose a otros trabajadores o clientes de la empresa o al público en general. Con muy variadas finalidades puede que el empresario quiera hacer públicos esos datos: ejemplaridad frente a los demás trabajadores, garantía de calidad para los clientes, promoción empresarial ante el público interesado, etc. No parece que este tratamiento de datos pueda tener el mismo fundamento que el que se agota en el exclusivo conocimiento del empresario. La AEPD ha tenido ocasión de pronunciarse sobre varios de estos supuestos.

La comunicación de estos datos al resto de trabajadores de la empresa es estudiada en el Informe 0529/2009 de la AEPD. Específicamente analiza la práctica empresarial consistente en comunicar verbalmente la productividad de un trabajador a sus compañeros, incluir en archivadores los resultados obtenidos por los trabajadores y publicarlos en la intranet de la empresa. Para la AEPD se trata de operaciones que implican tratamiento de datos personales pues los datos de los trabajadores “van a ser tratados no sólo por el empresario sino que van a ser cedidos a todos sus compañeros de trabajo”. La licitud del tratamiento de estos datos requerirá el consentimiento del trabajador, con todas las dificultades ya señaladas para perfi-

⁵⁴ BLÁZQUEZ AGUDO, E. M.: “La protección de datos en el desarrollo de la relación laboral”, en *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid, CISS, 2018, p. 2, citado según versión electrónica La Ley 2592/2018.

⁵⁵ PRECIADO DOMÉNECH, C.H.: *Los Derechos Digitales de las Personas Trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales*, Clzur Menor (Navarra), Aranzadi, 2019, p. 66.

⁵⁶ Recomendación 1/2001, sobre datos de evaluación de los trabajadores (22.3.2001), adoptada por el Grupo del Artículo 29. Citada en el Informe 0529/2009 de la AEPD, de donde se toma.

lar su libre prestación. Para la AEPD “la comunicación de datos relativos a la productividad de los trabajadores a otros trabajadores, ya sea mediante publicación de dichos datos en tablores, o en la intranet, deberá efectuarlo voluntariamente el trabajador, salvo que el Comité de Empresa se pronuncie considerando estas medidas como controles que efectúa el propio empresario a su trabajador al amparo del artículo 20.3 del Estatuto de los Trabajadores, en cuyo caso la cesión vendría amparada en el mencionado artículo”.

El Informe 0039/2010 de la AEPD trata de la publicación en la página web de la empresa de datos personales de sus trabajadores (identificación, fotografía, perfil profesional y aficiones), la evaluación de que han sido objeto por los clientes y la difusión por estos en las redes sociales. Para la AEPD “cabe concluir que el consentimiento para la comunicación masiva por Internet de los datos de sus empleados, incluidas las evaluaciones sobre los mismos, no podría entenderse válidamente prestado en el contexto de la relación laboral si sus negativa a darlo, llevase aparejada algún tipo de consecuencia adversa o discriminatoria, no pudiendo hablarse de consentimiento libre”. Por ello concluye que “la comunicación de los datos de los empleados en Internet, no puede ampararse en el consentimiento del trabajador, en el ámbito de la relación laboral”. Sobre la difusión de esos datos por los clientes en internet debe tenerse en cuenta que “la publicación de contenidos con información y datos respecto de terceros no puede ser realizada si éstos no han autorizado expresamente su publicación”.

La Resolución R/02223/2009 de la AEPD⁵⁷ resuelve la denuncia presentada frente a la empresa que publica en su tablón de anuncios, ubicado en un lugar al que tienen acceso trabajadores de otras empresas colaboradoras y clientes, un cuadro que contiene una relación de los trabajadores de la empresa junto con la valoración de sus conocimientos y eficacia en el puesto de trabajo. La empresa afirma que la

publicación de estos se justifica en el desarrollo de la relación laboral: se trata de facilitar y agilizar las suplencias de los trabajadores en los cambios de producción y de disponer de un baremo interno que mida la capacidad de los trabajadores. Se trataría, por tanto, de hacer frente a exigencias organizativas del trabajo en la empresa y de cumplimiento de la normativa de seguridad y prevención de riesgos laborales. Sin embargo la AEPD entiende que la publicación de estos datos es desproporcionada al permitir el acceso de terceros a dichos datos e implica una vulneración del deber de secreto: “por medio de un tablón de anuncios se ha difundido información de los trabajadores que revelan sus actitudes profesionales de cara a la realización de unas tareas determinadas, fuera de su ámbito adecuado y siendo accesibles a terceras personas, lo que implica una vulneración de dicho deber de secreto”.

4. RECOGIDA Y TRATAMIENTO DE DATOS EN LA EXTINCIÓN DEL CONTRATO DE TRABAJO

4.1. Los datos personales del trabajador despedido

La extinción del contrato de trabajo, sobre todo en los casos de despido, es un momento en el que normalmente se producirá el uso de datos personales del trabajador. El carácter causal del despido obliga a describir los hechos (art. 55.1 ET) o causas [art. 53.1.a) ET] que lo motivan, hechos o causas que, muy frecuentemente, consistirán en información sobre el trabajador despedido, otros trabajadores o terceros, es decir, datos personales. Algunos de esos datos personales de los trabajadores procederán de tratamientos anteriores efectuados en la empresa (filmaciones, grabaciones o registros de jornada para acreditar un incumplimiento contractual) con arreglo a las normas específicas previstas en el LOPDGD⁵⁸.

⁵⁷ PS/00118/2009.

⁵⁸ Arts. 87, 89 y 90 LOPDGD. Véanse los estudios correspondientes en este mismo número de la *Revista*.

Los problemas que se plantean en el momento del despido se refieren fundamentalmente a si el uso de los datos personales en la carta de despido y su necesaria comunicación a terceros en caso de impugnación judicial (jueces, peritos, otras partes, etc.) requieren el consentimiento del trabajador o se encuentran amparados por el mismo contrato de trabajo, pues el tratamiento es necesario para su extinción [art. 6.1.b) RGPD], o por el cumplimiento de una obligación legal [art. 6.1.c) RGPD], ya que es la ley la que obliga a incorporar a la carta de despido los hechos (art. 55.1 ET) o causas [art. 53.1.a) ET] que lo motivan.

Que no es necesario el consentimiento del trabajador despedido para proceder al tratamiento de los datos personales justificativos del despido queda claro en la SAN (CA) de 19 de octubre de 2005 (rec. 1139/2003)⁵⁹. El supuesto base fue el despido de un empleado de banca por disponer irregularmente en beneficio propio de fondos del banco. La entidad de crédito acreditó el incumplimiento contractual grave y culpable del trabajador mediante informes periciales y de su área de auditoría para cuya elaboración se usaron datos de carácter personal del despedido, entre otros los relativos a la utilización de su tarjeta de crédito y del contrato de préstamo que mantenía con la misma entidad. El trabajador denunció al banco por tratar sus datos personales sin su consentimiento, así como por revelarlos al juzgado, al personal del banco que elaboró el informe de auditoría y al perito. El tribunal estimó que no era necesario el consentimiento del trabajador pues las investigaciones realizadas por el banco a través de su servicio de auditoría interna y del informe pericial sobre las actuaciones del trabajador como empleado de la entidad “están vinculadas o afectan al mantenimiento y cumplimiento de la relación laboral existente entre ambos, exigiendo dicha relación un deber de lealtad y fidelidad que, al parecer o, al menos a juicio de la empleadora, fue incumplido por el referido trabajador” (FJ

3). También entendió el tribunal que no había cesión de datos en el acceso a los mismos por el servicio de auditoría (que es personal del responsable del fichero), juzgado, perito y abogados, justificado en el art. 11. LOPD-1999.

En los despidos por ineptitud [art. 52.a) ET] justificados de algún modo por la alteración de la salud del trabajador se ha planteado la cuestión de la suficiencia de la carta de despido cuando el empresario sólo incluye en ella la referencia a la calificación de ineptitud proporcionada por el servicio médico o de prevención correspondiente y no la descripción del proceso patológico. Aparecen aquí en tensión de un aparte, la necesaria suficiencia de la carta de despido que no deje en situación de indefensión al trabajador y de otra, no sólo el derecho a la protección de datos personales sino el mismo derecho a la intimidad del trabajador. Los datos de salud están sometidos a un régimen especial (art. 9 RGPD) y el art. 22 LPRL somete a los datos derivados de la vigilancia de la salud a una especial reserva: debe llevarse a cabo respetando el derecho a la intimidad del trabajador y la confidencialidad de toda la información relacionada con el estado de salud (art. 22.2 LPRL). Los “resultados” de los reconocimientos médicos serán comunicados al trabajador (art. 2.3 LPRL) y el acceso a la información médica se limitará al personal médico y a las autoridades sanitarias sin que pueda facilitarse al empresario o a terceros sin consentimiento expreso del trabajador (art. 22.4 LPRL). El empresario será informado de las “conclusiones” que se derive de los reconocimientos médicos en relación con la aptitud del trabajador para el desempeño del puesto de trabajo (art. 22.4 LPRL). El empresario sólo dispone de estas conclusiones, que es lo que puede aportar a la carta de despido. La STS de 22 de julio de 2005 (rec. 1333/2004)⁶⁰ proporciona un buen ejemplo de esta problemática. El supuesto se refiere al despido de un vigilante de seguridad al que el servicio de prevención declara no apto para el cumpli-

⁵⁹ JUR 2005, 268851.

⁶⁰ RJ 2006, 84.

miento de sus funciones de acuerdo con la normativa de seguridad privada. El empresario despidió al trabajador al amparo del art. 52.a) ET, sin que en la carta de despido conste la concreta alteración de salud inhabilitadora, sino sólo la conclusión de “no apto” del servicio de prevención de riesgos laborales. La cuestión que se plantea es si con sólo esa mención se cumple con el requisito de suficiencia de la carta de despido [art. 53.1.a) ET] sin generar indefensión del trabajador, la tensión entre intimidación y prohibición de indefensión del trabajador. La sentencia entiende que, ante la literalidad de la LPRL, el empresario no tiene otra opción sin que se cause indefensión al trabajador porque puede recabar del servicio de prevención los resultados de su reconocimiento médico. Cuestión distinta es que haya vinculación necesaria entre la declaración de “no apto” del servicio de prevención y la procedencia del despido: “la declaración de no apto por el servicio de prevención, propio o ajeno, no excusa al empleador de justificar la concurrencia de los requisitos legales del despido por ineptitud sobrevenida, para lo cual puede valerse de cualquiera de los medios de prueba admisibles a derecho, por ejemplo, citando ajuicio al facultativo que suscribió el informe declarando no apto al trabajador para que explique cuáles son las concretas dolencias que le aquejan y por qué no puede desempeñar sus funciones” [STSJ Aragón de 21 de febrero de 2018 (rec. 45/2018)⁶¹].

4.2. Datos personales de otros trabajadores

El tratamiento de datos personales de trabajadores distintos del despedido se ha planteado en algunos casos de despido colectivo (art. 51 ET) a propósito de la aplicación de los criterios seguidos para determinar los trabajadores que son despedidos. El interés del trabajador despedido en conocer la situación de otros trabajadores que no son despedidos reta

tanto al derecho a la protección de datos personales, pues sería un caso de comunicación de datos (art. 4.2 RGPD), como a la suficiencia de la carta de despido. En este contexto la STSJ País Vasco de 8 de abril de 2014 (rec. 527/2014)⁶² enjuicia el despido de un trabajador en un procedimiento de despido colectivo en el que el criterio para seleccionar a los despedidos era la menor capacidad o rendimiento en el puesto de trabajo, de acuerdo con la correspondiente evaluación interna, excluyéndose en todo caso quienes acreditaran una capacidad o rendimiento superiores al normal. El trabajador impugnó el despido alegando que en la carta de despido no se identificaba a los trabajadores que, pese a su menor antigüedad, acreditaban una capacidad o rendimiento superiores. Para la sentencia era innecesario que la carta de despido “detallara la concreta calificación obtenida por el demandante en el proceso de evaluación e identificara a los trabajadores con menor antigüedad a la suya que habían logrado la máxima, y menos aún que recogiera todos los datos reflejados en las correspondientes fichas, lo que además podría colisionar con lo dispuesto en los artículos 10 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”. En cualquier caso si el trabajador “tenía conocimiento de que la valoración negativa de su capacidad y rendimiento, y la positiva de los de otros trabajadores adscritos al mismo centro y grupo profesional, estaba basada en las hojas de evaluación realizadas por la empresa, como se reflejaba en el propio acuerdo suscrito con los representantes del personal, y en la carta de despido se le informaba de que era su menor capacidad y rendimiento respecto de otros compañeros que acreditaban la máxima, la determinante de su elección, ningún impedimento existía para que solicitase, por conducto judicial, la aportación por parte de la demandada, de la ficha de evaluación propia y de los demás trabajadores de la fábrica, incluso como prueba anticipada, al objeto de verificar la valoración con detalle

⁶¹ JUR 2018, 95275.

⁶² AS 2014, 830.

y rebatirla eficazmente a través de los medios de prueba adecuados a tal fin" (FJ 4).

4.3. Datos personales de terceros

No es infrecuente que en algunos despidos se plantee si datos personales de terceros, como los clientes de la empresa, deben acceder a la carta de despido. Piénsese, por ejemplo, en despidos por ofensas, daños o fraude a clientes o a otras personas. Un supuesto de este tipo fue resuelto por la STSJ Extremadura de 17 de noviembre de 2015 (rec. 464/2015)⁶³ al enjuiciar el despido disciplinario de un vendedor por las numerosas irregularidades cometidas en su trabajo. El trabajador despedido alegó indefensión porque la empresa no había incorporado en la carta de despido los nombres de los clientes afectados por las irregularidades sino solo el número asignado por la empresa. El tribunal declaró que la actuación empresarial había sido correcta y había cumplido con la LOPD-1999 pues se trataba de datos personales de terceros sobre los que la empresa estaba obligada a guardar secreto y además la empresa había comunicado al trabajador despedido que facilitaría los datos si el juzgado lo requiera: "actuó correctamente remitiéndole a quien puede determinar si procedía comunicar los datos sin necesidad de consentimiento de los clientes, al órgano judicial, como previene, según se dijo, el art. 11. Por ello, si el trabajador no hizo uso de esa posibilidad, en las diversas formas que, como se alega en la impugnación, le permitía la LRJS, no puede ahora achacar a la empresa las posibles consecuencias de su inacción" (FJ 2).

4.4. La comunicación del despido a terceros: "listas negras"

La STS (Civil) de 12 de noviembre de 2015 (rec. 899/2014)⁶⁴ aborda la cuestión de la co-

municación a terceros de los hechos, datos personales, motivadores del despido disciplinario, comunicación de datos hecha no con una simple y aséptica finalidad informativa sino con la de excluir al trabajador despedido de futuros empleos en otras empresas del sector, es decir, para formar una "lista negra"⁶⁵. Los hechos del caso fueron los siguientes. La subcontratista de una de las principales empresas del sector despidió a un trabajador, acusado de cobrar a un cliente por una actuación que debía ser gratuita. El despido fue declarado improcedente al no quedar acreditados los hechos imputados, optando el empresario por la extinción indemnizada del contrato. La empresa auxiliar comunicó a la principal los datos relativos a las causas del despido que quedaron incorporados a un fichero de "personal conflictivo" lo que imposibilitó la posterior contratación del trabajador por otras empresas auxiliares de la principal. La sentencia del Tribunal Supremo encuadra esta conducta empresarial dentro de la formación de las llamadas "listas negras"⁶⁶ cuya ilicitud declara por, entre otros, lesionar el derecho a la protección de datos personales: "Al tratarse de ficheros de datos personales formados sin el consentimiento de los afectados, en tanto no les fuera aplicable ninguna de las excepciones del art. 11.2 LOPD (RCL 1999, 3058), la cesión de datos que se hicie-

⁶⁵ MONEREO PÉREZ, J. L.; FERNÁNDEZ BERNAT, J. A.: "Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)", *Trabajo y Derecho*, núm. 16 (2016).

⁶⁶ La sentencia del Tribunal Supremo asume la definición del Grupo de Trabajo del Artículo 29: "ficheros de datos personales formados mediante la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación », entre las que destacan las que incluyen datos sobre la causa de suspensión o extinción de la relación laboral, existencia de reclamaciones judiciales contra la empresa efectuadas por el trabajador, así como si es susceptible de nueva contratación en función de respuestas a preguntas que no se concretan, extremos estos últimos que pueden afectar negativamente a la reputación del trabajador y a su futura empleabilidad " (FJ 3).

⁶³ JUR 2015, 297085.

⁶⁴ RJ 2015, 5063.

ra para la formación de tales ficheros sería ilícita, vulneraría el derecho fundamental a la protección de los datos personales y, si los datos objeto del tratamiento ilícito pudieran dañar el honor o la intimidad de los afectados, también constituiría una vulneración de estos derechos fundamentales de la personalidad” (FJ 3). Afirmada esta regla general la aplica al caso consistente en la comunicación por parte de la empresa auxiliar a la principal de datos personales del trabajador sobre las causas de su despido: “tal cesión de datos fue ilícita, porque no contó con el consentimiento del afectado, no resultaba amparada en ninguno de los supuestos en los que el art. 11.2 LOPD exime de la exigencia de consentimiento del afectado para que la cesión sea lícita, y, además, no respetaba el principio de calidad de datos pues los datos cedidos no eran veraces (la sentencia del Juzgado de lo Social los había considerado como no acreditados) y no se concedía al demandante la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, regulados en los arts. 15 a 17 LOPD” (FJ 4). De todo ello resulta la vulneración del derecho a la protección de datos, a la que se añade la del derecho al honor del trabajador “pues los datos comunicados no cumplían el requisito de la veracidad y afectaban negativamente a su reputación” (FJ 4).

4.5. Situación de los datos personales una vez extinguido el contrato de trabajo

Con la extinción del contrato de trabajo desaparecerá el fundamento principal del tratamiento de los datos del trabajador. A partir de ese momento ya no hay contrato cuya ejecución haga necesaria la recogida y tratamiento de datos [art. 6.1.b) RGPD]. El deber de confidencialidad del empresario se mantendrá aunque se hubiera extinguido el contrato (art. 5.3 LOPDGDD). Esos datos fueron recogidos con el fin determinado, el cumplimiento del contrato, que cesa con la extinción del contrato sin que sea posible su tratamien-

to ulterior de modo incompatible con dicho fin [art. 5.1.b) RGPD]. Conforme al art. 17.1 RGPD el trabajador tendrá derecho a obtener la supresión de sus datos personales cuando éstos “ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otros modos” [art. 17.1.a) RGPD]⁶⁷. El empresario, en estos casos, estará obligado a bloquear los datos (art. 32.1 LOPDGDD), operación consistente en la identificación y reserva de los datos “adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el pazo de prescripción de las mismas”. Pasado ese plazo “deberá procederse a la destrucción de los datos” (art. 32.2 y 3 LOPDGDD)⁶⁸.

Es claro que una vez extinguido el contrato de trabajo pueden plantearse reclamaciones judiciales o extrajudiciales del trabajador o actuaciones de las administraciones públicas por infracciones administrativas (de orden social, tributarias, protección de datos, etc.) que se refieran o deriven de datos personales del trabajador, por lo que se plantea la cuestión del plazo de conservación de los datos. Cada una de estas responsabilidades tiene plazo de prescripción distinto⁶⁹, por lo que parece que los datos deberían conservarse durante un plazo coincidente con el de más amplio contemplado por las normas en concurrencia⁷⁰.

⁶⁷ Art. 15.1 LOPDGDD.

⁶⁸ Para la normativa anterior, art. 16 LOPD-1999.

⁶⁹ Acciones derivadas del contrato de trabajo: (art. 59.1 ET). Infracciones en el orden social: art. 4 LISOS. Infracciones en materia de protección de datos: arts. 72.1, 73 y 74 LOPDGDD.

⁷⁰ En el caso de extinción de la relación laboral el empresario debe proceder al bloqueo de los datos “hasta que finalice el plazo de prescripción de acciones judiciales [TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010, p. 2 (citado según la versión electrónica del capítulo 13, “La protección de datos personales en el ámbito laboral”, en *tirantonline*)]. Según

El uso empresarial de datos personales de antiguos trabajadores de la empresa ha dado lugar a algunos litigios en los que se ha discutido la licitud de dicho tratamiento. La determinación del orden jurisdiccional competente para conocer las reclamaciones por vulneración del derecho a la protección de datos planteadas por antiguos trabajadores de la empresa se trató en la STSJ Andalucía (Sevilla) de 28 de septiembre de 2017 (rec. 2762/2017)⁷¹. La AEPD consideró infracción grave la conducta de la empresa que envió ofertas comerciales a antiguos trabajadores utilizando los datos que había obtenido por la previa y extinta relación laboral, sin que los trabajadores hubieran autorizado su uso para finalidad distinta [art. 44.3.b) LOPD-1999]. Planteada reclamación judicial ante los tribunales del orden social por vulneración del derecho fundamental a la protección de datos la sentencia indicada declaró que una vez concluida la relación laboral el empresario seguía obligado a “respetar los derechos fundamentales de los actores pero no en la condición de trabajadores de la empresa, que ya no ostentan ni conforme a lo dispuesto en las normas laborales y a la doctrina constitucional sobre el contenido y límites de los derechos fundamentales en el marco de una relación de esa naturaleza, sino como personas que podrán recabar la tutela judicial

frente a la actuación que consideran lesiva de su derecho fundamental a la protección de datos por la vía privilegiada del artículo 53.1 CE, no ante los tribunales laborales, que carecen de competencia para conocer de las demandas de tutela de los derechos fundamentales que se suscitan fuera del ámbito de la relación de trabajo, aunque tengan una conexión más o menos próxima con una previa relación laboral, sino ante los del orden civil, en ejercicio del derecho a la tutela judicial efectivo reconocido por el artículo 24.1 CE” (FJ 2).

En algún caso el tratamiento de datos una vez extinguido el contrato se hace con la finalidad de evitar conductas desleales de los antiguos trabajadores. Así fue en el supuesto que dio lugar a la SAN (CA) de 15 de junio de 2005 (rec. 669/2003)⁷². Tras la creación de una sociedad por antiguos trabajadores de un distribuidor el fabricante, utilizando los datos de los antiguos trabajadores facilitados por el distribuidor y a petición suya, comunicó a sus clientes no guardaba relación alguna con la nueva sociedad formada por los antiguos trabajadores. Esta conducta fue sancionada como infracción administrativa grave por utilizar los datos personales de los trabajadores con finalidad distinta para la que se recogieron [art. 44.3.d) LOPD-1999]. Sin embargo la AN estimó que los datos no se habían utilizado “con una finalidad distinta de aquella para la que habían sido recabados”, pues se utilizaron para una “finalidad derivada, o al menos directamente relacionada de dicha relación laboral” porque al extinguirse los contratos de trabajo la empresa “trató de evitar los perjuicios que le podía suponer una posible competencia desleal de aquellos antiguos trabajadores, al servirse de la cartera de clientes de dicha empleadora, y por en consecuencia puede considerarse “compatible” con dicha relación laboral el enviar una carta a los clientes de la empresa advirtiéndoles del cese en ella de tales trabajadores” (FJ 4).

PRECIADO DOMÉNECH “parece que los datos de los trabajadores deberían bloquearse a la extinción del contrato, conservarse bloqueados durante 4 años y suprimirse después” (*El derecho*, cit., p. 294); conclusión a la que llega tras ponderar los plazos de prescripción de las infracciones de la LOPD-1999 (tres años), tributarias (cuatro años, art. 66 LGT), de seguridad social (cuatro años, art. 4.2 LISOS) y la regla general de las infracciones de orden social (tres años, art. 4.1 LIOSOS). Pero téngase en cuenta que las infracciones muy graves en materia de prevención riesgos laborales prescriben a los cinco años (art. 4.3 LPRL). Para MERCADER UGUINA “de forma orientativa, se ha venido señalando que dicho período coincidirá típicamente con el tiempo necesario para la prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al responsable con el interesado” (MERCADER UGUINA, J. R.: “Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679”, [La Ley 3360/2018, p. 15, versión digital]).

⁷¹ JUR 2017, 263201.

⁷² JUR 2005, 240213.

BIBLIOGRAFÍA

- ARIAS DOMÍNGUEZ, Á.: “Video-llamadas en trabajos de contact-center y cesión de derechos de imagen”, *Revista de Jurisprudencia Laboral*, núm. 3 (2019).
- BLÁZQUEZ AGUDO, E. M.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid, CISS, 2018.
- CANO GALÁN, Y.: “Cláusulas contractuales tipo sobre cesión de derechos de imagen de los trabajadores y cumplimiento de la normativa sobre protección de datos de carácter personal”, *Diario La Ley*, 24 de Mayo de 2018 (LA LEY 7684/2019).
- COSTA, R.: “Protección de datos en el ámbito laboral”, en RALLO LOMBARTE, A.: *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019.
- CRISTÓBAL RONCERO, R.: “Protección del derecho a la propia imagen en el trabajo”, *Nueva Revista Española de Derecho del Trabajo*, núm. 199 (2017).
- DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Valladolid, Lex Nova, 2012.
- GARCÍA MURCIA, J.: “La protección de datos personales en el ámbito laboral: una sucinta reseña jurisprudencial a partir de cinco sentencias del Tribunal Supremo”, *Revista Galega de Dereito Social*, núm. 5 (2018).
- GARCÍA MURCIA, J.; RODRÍGUEZ CARDO, I. A.: “La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo”, *Revista Española de Derecho del Trabajo*, núm. 216 (2019).
- GARCÍA-PERROTE ESCARTÍN, I.; MECADER UGUINA, J. R.: “Datos personales y cláusulas contractuales: los límites del consentimiento en la doctrina reciente del Tribunal Supremo”, *Revista Española de Derecho del Trabajo*, núm. 223 (2019).
- MARTÍNEZ MARTÍNEZ, R.: “El derecho fundamental a la protección de datos: perspectivas”, *Revista de Internet, Derecho y Política*, núm. 5 (2007).
- MARTÍNEZ MOYA, J.: “El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores”, *Revista de Jurisprudencia Laboral*, núm. 1 (2019).
- MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª ed., Madrid, Lefebvre, 2019.
- : “Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679”, (La Ley 3360/2018).
- MERCADER UGUINA, J. R.; DE LA PUEBLA PINILLA, A.: “Protección de datos y relaciones colectivas”, *Revista de Trabajo y Seguridad Social. CEF*, núm. 423 (2018).
- MESSÍA DE LA CERDA BALLESTEROS, J. A.: “La evolución del concepto de cesión o comunicación de datos personales”, *Actualidad Civil*, núm. 10 (2017).
- MONEREO PÉREZ, J. L.; FERNÁNDEZ BERNAT, J. A.: “Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)”, *Trabajo y Derecho*, núm. 16 (2016).
- OLLERO TASSARA, A.: *De la protección de la intimidad al poder de control sobre los datos personales*, Madrid, Real Academia de Ciencias Morales y Políticas, 2008.
- PRECIADO DOMENECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Cizur Menor (Navarra), Aranzadi, 2017.
- : *Los Derechos Digitales de las Personas Trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales*, Cizur Menor (Navarra), Aranzadi, 2019.
- RODRÍGUEZ ESCANCIANO, S.: “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Revista de Trabajo y Seguridad Social CEF*, núm. 423 (2018).
- RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009.
- SAN MARTÍN MAZZUCCONI, C.: “El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos”, en SAN MARTÍN MAZZUCCONI, C. (Dir.): *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, León, Eolas, 2014.
- SÁNCHEZ QUINONES, L.: “El marco legislativo de la protección de datos en el ámbito laboral. Especial referencia al consentimiento del trabajador”, *Diario La ley*, núm. 9377 (2019).
- SEMPERE NAVARRO, A. V.: “El deber de facilitar una cuenta corriente bancaria”, *Revista de Jurisprudencia Laboral*, núm. 7 (2019).
- TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010.
- VILLALBA SÁNCHEZ, A.: “El derecho fundamental a la protección de datos del trabajador frente a los riesgos de la contratación estandarizada”, *Nueva Revista Española de Derecho del Trabajo*, núm. 207 (2018).

RESUMEN

El derecho fundamental a la protección de datos encuentra una de sus más importantes aplicaciones en el ámbito de la relación laboral. Su ciclo vital (selección, contratación, cumplimiento y extinción) permite y exige disponer de una información masiva sobre el trabajador, de un elevadísimo número de datos personales sobre sus más variadas circunstancias. De este modo resulta que: a) Sería imposible la celebración, cumplimiento y extinción del contrato de trabajo sin la disposición de datos personales de los trabajadores. b) Estos actos suponen la disposición del derecho fundamental a la protección de datos, un capítulo más del tema de la vigencia de los derechos fundamentales inespecíficos del trabajador en el contrato de trabajo. c) De los dos elementos anteriores, necesidad del tratamiento de datos personales para el desenvolvimiento de la relación laboral y atribución al trabajador de un poder de disposición y de control sobre los mismo configurado como derecho fundamental, resultará la modulación del derecho fundamental a la protección de datos.

La protección de datos personales se convierte así en un punto de vista desde el que el Derecho del Trabajo, y particularmente el contrato de trabajo, puede ser mirado en su integridad. A la luz de este derecho fundamental, entre el trabajador, como “interesado”, y el empresario, como “responsable del tratamiento” de los datos personales, se anudan un complejo conjunto de derechos y obligaciones. De ese amplio conjunto de obligaciones y derechos corresponde a este trabajo el estudio de la recogida y tratamiento de datos personales en el contexto del contrato de trabajo. Como en otros artículos de este volumen se estudian destacados aspectos generales y específicos del derecho a la protección de datos en las relaciones laborales, para evitar innecesarias y tediosas reiteraciones, se ha optado por presentar en estas páginas un sucinto análisis de la casuística más destacada generada por la recogida y tratamiento de datos en el contexto del contrato de trabajo. Siguiendo la estructura habitual de los principales estudios publicados sobre el tema estas páginas se estructura en tres grandes apartados, según la recogida y tratamiento de datos personales de los trabajadores se produzca: 1) en el momento de la celebración del contrato de trabajo; 2) durante su cumplimiento, y 3) en su extinción.

La celebración del contrato de trabajo es un momento en el que se concentra de modo importante la recogida y tratamiento de datos personales de los trabajadores. El mismo contrato de trabajo puede ser instrumento útil para el cumplimiento de dos importantes funciones: recabar el consentimiento del trabajador para el tratamiento de los datos e informarle sobre el tratamiento realizado. El principal criterio de licitud para el tratamiento de los datos personales en este momento es el de su necesidad para la ejecución del contrato de trabajo del que el trabajador es parte. De este modo el consentimiento del trabajador pasa, como regla general, a un segundo plano. No es necesario, por tanto, recurrir al principio del consentimiento del interesado para hacer lícito el tratamiento de estos datos indispensables para la celebración y posterior ejecución del contrato de trabajo. Por otra parte la normativa de protección de datos personales contempla con muchas restricciones la prestación del consentimiento del trabajador para el tratamiento de sus datos personales, habida cuenta de su situación de debilidad contractual. Se trata de una cuestión que ha dado lugar a una cierta litigiosidad en la que se puede apreciar dos grandes grupos de casos. Uno en el que los datos personales para cuyo tratamiento se presta el consentimiento no guardan relación con el objeto del contrato de trabajo y otro en el que los datos personales sí están implicados en la prestación laboral del trabajador. En el primer caso no se considera válida la prestación del consentimiento, en el segundo sí. También se estudia en esta primera parte el tratamiento de datos necesario para el cumplimiento de obligaciones legales del empresario, fundamentalmente la entrega de la copia básica del contrato a los representantes de los trabajadores.

La segunda parte del estudio se dedica al análisis de la recogida y tratamiento de datos durante el cumplimiento del contrato de trabajo. Fundamentalmente es objeto de estudio el flujo de datos personales de los trabajadores que se produce entre empresarios y clientes intervinientes en relaciones negociales: identificación de los trabajadores ante los clientes, comunicación de salarios y cotizaciones a la seguridad social por el empresario auxiliar al principal, externalización de la gestión de personal y *data outsourcing*. Finalmente se plantea en este apartado las consecuencias que desde el punto de vista de la protección de datos tienen las prácticas empresariales de evaluación del desempeño de los trabajadores y su comunicación a clientes y compañeros de trabajo.

La última parte se dedica al estudio del tratamiento de datos personales que se puede producir con ocasión de la extinción de la relación laboral. La extinción del contrato de trabajo, sobre todo en los casos de despido, es un momento en el que normalmente se producirá el uso de datos personales del trabajador. El carácter causal del despido obliga a describir los hechos que lo motivan, hechos o causas que, muy frecuentemente, consistirán en información sobre el trabajador despedido, otros trabajadores o terceros, es decir, datos personales. Los problemas que se plantean en el momento del despido se refieren fundamentalmente a si el uso de los datos personales en la carta de despido y su necesaria comunicación a terceros en caso de impugnación judicial requieren el consentimiento del trabajador o se encuentran amparados por el mismo contrato de trabajo, pues el tratamiento es necesario para su extinción, o por el cumplimiento de una obligación legal, ya que es la ley la que obliga a incorporar a la carta de despido los hechos o causas que lo motivan. Finalmente se estudia la situación producida una vez extinguido el contrato de trabajo al desaparecer el fundamento principal del tratamiento de los datos del trabajador. A partir de ese momento ya no hay contrato cuya ejecución haga necesaria la recogida y tratamiento de datos. El deber de confidencialidad del empresario se mantendrá aunque se hubiera extinguido el contrato. Esos datos fueron recogidos con el fin determinado, el cumplimiento del contrato, que cesa con la extinción del contrato sin que sea posible su tratamiento ulterior de modo incompatible con dicho fin, abriéndose los procesos de bloqueo y destrucción de datos.

Palabras clave: datos personales; derechos fundamentales; derecho a la protección de datos; relación laboral.

ABSTRACT

The fundamental right to data protection finds one of its most important applications in the field of labor relations. Its life cycle (selection, hiring, compliance and extinction) allows and demands to have a massive information about the worker, a very high number of personal data about his most varied circumstances. Thus it turns out that: a) It would be impossible to conclude, fulfill and terminate the employment contract without the provision of personal data of the workers. b) These acts involve the provision of the fundamental right to data protection, another chapter on the issue of the validity of the nonspecific fundamental rights of the worker in the employment contract. c) Of the two previous elements, the need for the processing of personal data for the development of the labor relationship and attribution to the worker of a power of disposition and control over the same configured as a fundamental right, will result the modulation of the fundamental right to protection of data.

The protection of personal data thus becomes a point of view from which Labor Law, and particularly the employment contract, can be viewed in its entirety. In light of this fundamental right, between the worker, as “interested”, and the employer, as “responsible for the processing” of personal data, a complex set of rights and obligations are tied. Of this broad set of obligations and rights corresponds to this paper the study of the collection and processing of personal data in the context of the employment contract. As in other articles of this volume are studied outstanding general and specific aspects of the right to data protection in labor relations, to avoid unnecessary and tedious repetitions, we have chosen to present in these pages a succinct analysis of the most outstanding casuistry generated for the collection and processing of data in the context of the employment contract. Following the usual structure of the main studies published on the subject, these pages are structured in three main sections, depending on the collection and processing of personal data of the workers: 1) at the time of the conclusion of the employment contract; 2) during its fulfillment, and 3) in its extinction.

The conclusion of the employment contract is a time in which the collection and processing of personal data of workers is concentrated. The same employment contract can be a useful instrument for the fulfillment of two important functions: to obtain the consent of the worker for the treatment of the data and to inform him about the treatment carried out. The main criterion of legality for the processing of personal data at this time is that of their need for the execution of the employment contract to which the worker is a party. In this way the worker's consent, as a general rule, goes to the background. It is not necessary, therefore, to resort to the principle of the consent of the interested party to make lawful the processing of these essential data for the conclusion and subsequent execution of the employment contract. On the other hand, the personal data protection regulations contemplate with many restrictions the provision of the worker's consent for the processing of their personal data, given their situation of contractual weakness. This is an issue that has given rise to a certain litigation in which you can see two large groups of cases. One in which the personal data for which the consent is given is not related to the object of the employment contract and the other in which the personal data is involved in the worker's labor benefit. In the first case the provision of consent is not considered valid, in the second case. In this first part, the treatment of data necessary for the fulfillment of legal obligations of the employer is also studied, mainly the delivery of the basic copy of the contract to the workers' representatives.

The second part of the paper is dedicated to the analysis of the collection and processing of data during the fulfillment of the employment contract. Fundamentally, the flow of personal data of workers that occurs between employers and clients involved in business relationships is studied: identification of workers before clients, communication of salaries and social security contributions by the auxiliary employer to the principal, outsourcing of personnel management and data outsourcing. Finally, this section considers the consequences that, from the point of view of data protection, business practices have to assess the performance of workers and their communication to customers and co-workers.

The last part is dedicated to the study of the processing of personal data that may occur during the termination of the employment relationship. The termination of the employment contract, especially in cases of dismissal, is a time when the use of personal data of the worker will normally occur. The causal nature of the dismissal makes it necessary to describe the facts that motivate it, facts or causes that, very frequently, will consist of information about the dismissed worker, other workers or third parties, that is, personal data. The problems that arise at the time of dismissal refer fundamentally to whether the use of personal data in the letter of dismissal and its necessary communication to third parties in case of judicial challenge require the consent of the worker or are covered by the same contract of work, because the treatment is necessary for its extinction, or for the fulfillment of a legal obligation, since it is the law that forces to incorporate to the letter of dismissal the facts or causes that motivate it. Finally, the situation produced after the employment contract is terminated when the main basis of the worker's data processing disappears. From that moment there is no contract whose execution makes the collection and processing of data necessary. The employer's duty of confidentiality will be maintained even if the contract has been terminated. These data were collected for the purpose determined, the fulfillment of the contract, which ceases with the termination of the contract without further processing in a manner incompatible with that purpose, opening the processes of blocking and destruction of data.

Keywords: personal data; fundamental rights; right to data protection; employment relationship.