DIGITALIZACIÓN Y PROTECCIÓN DE DATOS DE LAS PERSONAS TRABAJADORAS: ESPECIAL REFERENCIA AL DELEGADO DE PROTECCIÓN DE DATOS

Laura Melián Chinea*
Universidad de La Laguna

Resumen

La mayoría de las empresas, con independencia de su tamaño o sector al que pertenecen, digitalizan las relaciones laborales. Las organizaciones operan en una economía datificada, donde los trabajadores digitales no solo prestan servicios bajo la dirección y control de empresas virtuales, sino que ceden gratuitamente su información personal en beneficio de estas entidades. Debido a los nuevos desafíos que presenta la inteligencia artificial en la gestión de los recursos humanos, el presente estudio analiza el marco normativo vigente a nivel europeo y nacional que trata de preservar la privacidad en el entorno laboral y garantizar la autonomía individual de la persona trabajadora, la cual inspira todo sistema democrático de relaciones laborales. Para un tratamiento adecuado de los datos personales de las personas trabajadoras se ha creado la figura del delegado de protección de datos, cuyo nombramiento es fundamental para evitar que plataformas digitales operen al margen de la legalidad.

Palabras clave: digitalización, relaciones laborales, plataformas digitales, protección de datos, derechos fundamentales.

DIGITIZATION AND DATA PROTECTION OF WORKERS' DATA: PARTICULAR REFERENCE TO THE DATA PROTECTION OFFICER

Abstract

Most companies, regardless of their size or sector, digitize labor relations and operate in an economy of data. Digital workers not only provide services under the management and control of virtual companies, but also freely give away personal information for the benefit of these organizations. Due to the new challenges presented by artificial intelligence in human resource management, this study analyzes the current international and national regulatory framework that seeks to preserve privacy in the work environment and guarantee the individual autonomy of the worker, which inspires any democratic system of labor relations. For an effective treatment of employees' personal data, the figure of the data protection officer has been created, whose appointment is essential to prevent digital platforms operate outside the law.

Keywords: Digitization, labor relations, digital platforms, data protection, fundamental rights.

DOI: https://doi.org/10.25145/j.anfade.2022.39.03
Anales de la Facultad de Derecho, 39; julio 2022, pp. 49-61; ISSN: e-2530-8319

1. LA MERCANTILIZACIÓN DE LOS DATOS PERSONALES EN LA ERA DEL TRABAJO DIGITAL

El mercado global actual se caracteriza por la interacción constante entre Estado, capital y sociedad en un contexto de hipertecnologización[1]. El auge de las *Big Tech*[2] ha propiciado la creación de un nuevo modelo productivo que radica en la extracción y sistematización de datos. Este modelo, denominado capitalismo de la vigilancia o de la información, da a luz a una nueva especie de poder instrumental que tiene la capacidad de conocer el comportamiento humano y orientarlo hacia los fines de otros[3]. En la actualidad, los capitalistas conciben al individuo como un agente económico cuyas decisiones generan *per se* riqueza[4].

La información personal es una fuente de ingresos y «las compañías que recolectan y procesan nuestros datos tienen las valoraciones económicas más altas de la historia»[5]. Ante este escenario, se ha considerado desde las instancias europeas que la transferencia de datos debería estar sujeta a tipos impositivos en la medida en que constituyen auténticos beneficios monetarios[6].

La digitalización de las relaciones laborales favorece al capitalismo de la información. Por ello, la mayoría de las empresas, con independencia de su tamaño o sector al que pertenecen, digitalizan las relaciones laborales y operan en una economía datificada[7]. La analítica de las personas es una subciencia de la minería de

---

* Profesora ayudante doctora de Derecho del trabajo y de la seguridad social de la Universidad de La Laguna.

[1] Jiménez González, A. y Menéndez de Llano, C.R., «Capitalismo digital: fragilidad social, explotación y solucionismo tecnológico», *Revista de Cultura Digital y Movimientos Sociales*, n.º 17, 2020, p. 98.

[2] Es el caso de «gigantes informáticos» como Google, Facebook, Uber, Glovo, Apple, Deliveroo, Amazon, Microsoft, entre otros.

[3] Soshana, Z., *La era del capitalismo de la vigilancia*, Paidós, Barcelona, 2020, p. 22.

[4] Harari, Y., *21 lecciones para el siglo xxi*, PRHGE, Barcelona, 2022, p. 77.

[5] Informe de UGT, *Guía para comprender el nuevo capitalismo de datos, la economía de plataformas y sus riesgos,* 2021, disponible en https://www.ugt.es/sites/default/files/guia-algoritmos_ediciondigital.pdf.

[6] La propuesta de Directiva del Consejo Europeo en el año 2018 refleja la preocupación por la contribución personal de los usuarios en las empresas «Big Tech», que se traducen en la creación de riqueza empresarial no sujeta a ningún tipo de gravamen. Propuesta de Directiva del Consejo relativa al sistema común del impuesto sobre los servicios digitales que grava los ingresos procedentes de la prestación de determinados servicios digitales, Bruselas, 21.3.2018 COM (2018) 148 final. En este sentido, véase la ley 4/2020, de 15 de octubre, del Impuesto sobre Determinados Servicios Digitales.

[7] Según un informe detallado sobre la economía de plataformas elaborado por el Instituto Sindical Europeo (2022) se estima que, tras varias encuestas realizadas en el año 2021, prestaron servicios digitales 47,5 millones de trabajadores en Internet y 12 millones de trabajadores prestaron servicios de forma exclusiva para plataformas. El informe «Deep Digital Journey» aporta numerosas evidencias relevantes para conocer la evolución del proceso de digitalización de grandes compañías con sedes repartidas en diferentes partes del mundo. El 45% de las empresas encuestadas afirma disponer de datos en la nube para activar sus estrategias y tomar decisiones, Véase el informe *Deep Digital*

datos que permite la gestión y evaluación de los recursos humanos[8]. El tratamiento de datos personales se produce durante todo el proceso de la relación laboral, desde la fase previa a la contratación hasta la extinción del contrato de trabajo. La experiencia humana de las personas trabajadoras se convierte así en una materia prima gratuita para el incremento de los beneficios empresariales.

La transformación de las empresas en el marco de la quinta revolución industrial es una cuestión de competitividad en un mundo marcado por la globalización y por las consecuencias negativas de la pandemia. De hecho, las organizaciones que se encuentran en una fase avanzada de la digitalización crecen de forma vertiginosa, al contrario que otras empresas[9]. Además, entre las compañías más exitosas, las líderes del sector son aquellas que tienen un mayor número de trabajadores digitales[10], pues el éxito empresarial responde a una doble prestación por la parte más débil del contrato de trabajo: en primer lugar, la realización de una obra o servicio; en segundo lugar, la transmisión inconsciente de información privada. En otros términos, los trabajadores digitales no solo prestan un servicio por cuenta ajena en las plataformas (empresario virtual), sino que ceden gratuitamente información personal, incrementando los beneficios de la empresa para la cual ya trabajan.

Por otro lado, la datificación del mercado laboral permite un control mucho más incisivo que va más allá de la vigilancia del cumplimiento de las obligaciones laborales[11]. A modo de ejemplo, la instalación de dispositivos de seguimiento es muy habitual en organizaciones cuya actividad incluya el transporte. Diversas aplicaciones informáticas incorporan sistemas de localización que informan detalladamente sobre la ubicación de la persona trabajadora, además de proporcionar otra información relativa a la conducción, como el trayecto y la velocidad. Los registradores de datos son especialmente invasivos cuando informan al empleador sobre acontecimientos muy concretos. Ante esta situación, la Agencia Española de Protección de Datos (en adelante AEPD) ha manifestado, en la guía de protección de datos (2021), que la geolocalización es un mecanismo lícito de vigilancia siempre que: a) permita

---

Journey. El viaje hacia la transformación digital de las compañías, Madrid, 2021, disponible en https://www.itseller.cl/wp-content/uploads/2021/11/211022_Deep-Digital-Journey_ES.pdf.

[8] Rivas Vallejo, P., «La gestión analítica de personas en la era digital: su impacto sobre los derechos fundamentales», en AA. VV., *De la economía digital a la sociedad del e-work decente: condiciones sociolaborales para una industria 4.0 justa e inclusiva* (dir. por Molina Navarrete y Vallecillo Gámez), Thomson Reuters, Aranzadi, Navarra, 2021, p. 263.

[9] El informe realiza esta distinción: las personas trabajadoras de internet prestan un servicio digital más amplio, su actividad no se limita a una plataforma en concreto; las personas trabajadoras de plataformas desarrollan una actividad más específica, realizando un tipo de trabajo en una específica plataforma, Piasna, A., Drahokoupil, J. y Zwysen, W., *The platform economy in Europe*, Results from the second ETUI Internet and Platform Work Survey, Bruselas, 2022, p. 52.

[10] «Las empresas de sectores líderes tienen una fuerza de trabajo 13 veces más digitalizada que el resto de la competencia», en Vidal, M., *La era de la humanidad. Hacia la quinta revolución industrial*, Deusto, Barcelona, 2020, p. 197.

[11] López Balaguer, M. y Ramos Moragues, F., «Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad», *LexSocial*, vol. 10, n.º 2, p. 509.

hacer un seguimiento sobre las herramientas que sean propiedad de la empresa como vehículos y dispositivos móviles, b) el tratamiento de datos responda a los principios de proporcionalidad y subsidiariedad, c) persiga un fin profesional específico y d) se informe sobre su utilización a las personas trabajadoras[12].

Debido a la mencionada datificación impulsada por el capitalismo de la vigilancia, la digitalización de las relaciones laborales podría colisionar con la protección de determinados derechos fundamentales. El recurso a las nuevas tecnologías, especialmente la aplicación de sistemas algorítmicos, propicia un nuevo conflicto ente la libertad de empresa y el derecho a la privacidad en el marco de la era digital. El Derecho del Trabajo se enfrenta a una sociedad digital que impacta sobre un conjunto de derechos y libertades de la persona. De conformidad con el compromiso de los poderes públicos de promover las condiciones necesarias para que la libertad y la igualdad de la persona sean reales y efectivas, el primer paso sería garantizar y hacer extensibles en el entorno digital los derechos fundamentales reconocidos en la Sección Primera del Capítulo Segundo del Título I de la Constitución española, así como los principios rectores de la política social y económica recogidos en el Capítulo Tercero del mismo título[13].

2. LA PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL: RÉGIMEN JURÍDICO APLICABLE

2.1. La intimidad informática: un derecho fundamental inespecífico

Los diversos cambios políticos, sociales, económicos y fundamentalmente tecnológicos han amenazado la esfera privada de la persona. La intimidad no puede ser entendida como un concepto hermético, sino abierto a las circunstancias del tiempo y del espacio donde se inserta[14]. Con independencia de la evolución del concepto del derecho a la intimidad, su contenido implica dos poderes: por un lado, la facultad de la persona de impedir la obtención de información personal injustificada o intrusiva; y, por otro lado, la facultad de oponerse a la divulgación ilegítima de sus datos[15].

En el marco de la digitalización de las relaciones laborales, las personas trabajadoras tienen derecho a preservar su intimidad ante las nuevas facultades de dirección y control empresarial favorecidas por las innovaciones tecnológicas. Ante

[12] Guía para la protección de datos en las relaciones laborales, elaborada por la Agencia Española de Protección de Datos en las Relaciones Laborales (AEPD), 2021, p. 56.

[13] Piñar Mañas, J.L., «Derecho e innovación. Privacidad y otros derechos en la sociedad digital», en AA. VV., *El derecho a la protección de datos personales en la sociedad digital* (coord. por Casas Baamonde), Fundación Ramón Areces, Madrid, 2020, p. 43.

[14] Cardona Rubert, M.B., «El derecho a la intimidad en la relación laboral. información relativa al trabajador», *Ius et Praxis*, n.º 4, 1998, p. 108.

[15] Goñi Sein, J.L., «El SIDA y el lugar de trabajo», *Relaciones Laborales*, n.º 17, 1997, p. 52.

este escenario, surge el derecho a la intimidad informática como un derecho de tercera generación[16], autónomo e independiente –imbricado, a su vez, en el derecho constitucional a la intimidad– que responde a las nuevas amenazas, retos y desafíos en la era del *Big Data*.

La norma suprema del ordenamiento jurídico español reconoce en su art. 18.4 el derecho a la protección de datos personales y garantiza el control personal de los mismos, al establecer que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». De la definición constitucional de dicho art. 18.4 CE, emerge, de su núcleo esencial, «el derecho del afectado a ser informado de quién posee los datos personales y, especialmente por lo que a los presentes efectos interesa, con qué fin son utilizados»[17]. A pesar de compartir contenido con el derecho a la intimidad previsto en el art. 18.1 CE, cuya finalidad es proteger a la persona frente a cualquier invasión que pueda realizar en el ámbito de la vida personal y familiar, el derecho a la intimidad informática constituye una garantía adicional al asegurar a la persona un control de sus datos personales (*habeas data*)[18]. Como así ha manifestado el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre:

> con la inclusión del vigente art. 18.4 C.E. el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía «como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona».

La protección de la privacidad en la era digital preserva la autonomía individual que inspira todo sistema democrático de relaciones laborales. Debido a que su tutela es el presupuesto fundacional de una sociedad libre[19], la intimidad informática debe configurarse como un derecho fundamental inespecífico que requiere de la máxima protección jurídica. De conformidad con el art. 53.2 CE, cualquier ciudadano puede recabar su tutela ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

---

[16] Olarte Encabo, S., «La aplicación de inteligencia artificial a los procesos de selección de personal y ofertas de empleo: impacto sobre el derecho a la no discriminación», *Documentación Laboral*, n.º 119, 2020, p. 84.

[17] La STS 889/2022, de 8 de marzo (rec. 130/2019) recoge la doctrina del Tribunal Constitucional (SSTC 57/1994; 18/1999; 98/2000; 292/2000; 308/2000 y 29/2013).

[18] Véase el comentario de sentencia realizado por Rodríguez Crespo, M.J., «El derecho a la intimidad informática del trabajador: un límite más al poder de dirección del empresario», *Temas laborales*, n.º 128, 2015, p. 212.

[19] Nieves Saldaña, M., «El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego», *UNED, Teoría y Realidad Constitucional*, n.º 28, 2011, p. 287.

Ahora bien, tal y como ha señalado la doctrina del Tribunal Constitucional[20], el derecho fundamental a la intimidad informática no es absoluto

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

2.2. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, general de protección de datos

Tanto la Carta de los Derechos Fundamentales de la Unión Europea (art. 8.1) como el Tratado de Funcionamiento de la Unión Europea (art. 16.1) manifiestan, en los mismos términos, que toda persona tiene derecho a la protección de los datos de carácter personal. Además, el segundo texto realiza un llamamiento al Parlamento Europeo y al Consejo para que establezcan, a través del procedimiento legislativo correspondiente, las normas sobre protección de las personas físicas respecto del tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros. Con objeto de proporcionar una regulación homogénea en toda la Unión Europea, se aprueba el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, general de protección de datos (en adelante, RGPD). Esta normativa europea proporciona seguridad jurídica, pues además exige que cada Estado miembro se dote de una infraestructura administrativa que permita controlar adecuadamente su cumplimiento (art. 57 RGPD). En España, la condición de autoridad la ostenta la Agencia Española de Protección de Datos (en adelante, AEPD).

De conformidad con el art. 4.1 del RGPD, se considera «dato personal» toda aquella información que puede asociarse a una persona identificada o identificable, como el nombre y apellido, nacimiento, domicilio, estado civil, número de identificación, entre otros. Una persona es identificada cuando el dato permita distinguir a la misma dentro de un grupo o colectivo. En cambio, una persona es identificable cuando el dato permite determinar la identidad[21]. Por tanto, como así ha declarado el TJUE en su Sentencia de 6 de noviembre de 2003 (asunto C-101/01),

> La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales».

[20] Véase la STC 186/2000, de 10 de julio.

[21] De val Tena, A.L., «La protección de datos personales en los procesos de selección de los trabajadores; en particular, aquellos datos especiales», *Documentación laboral*, n.º 119, 2020, p. 109 y ss.

En el marco de los datos personales, merecen especial atención aquellos datos previstos en el art. 9.1 del RGPD. Estos integran la categoría de «datos especiales» por revelar el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física como imágenes faciales o huellas dactilares y los datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física.

Se trata de información sensible por pertenecer a la esfera privada de la persona y que, por ende, requiere de una mayor protección jurídica. Por este motivo, su tratamiento está expresamente prohibido por la normativa europea con carácter general, salvo que el interesado consienta de manera explícita su tratamiento para fines determinados o se requiera para atender supuestos específicos, destacando en el ámbito de las relaciones de trabajo los siguientes: el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado; el ejercicio de funciones sindicales en el ámbito de sus actividades legítimas y con las debidas garantías, siempre que el tratamiento de datos se refiera exclusivamente a los afiliados y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; y la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial. En estas circunstancias deben aplicarse los principios generales y otras normas del presente Reglamento como la licitud del tratamiento. En todo caso, el Reglamento no excluye el Derecho de los Estados miembros a mantener o introducir condiciones adicionales, inclusive restricciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

La relevancia de la protección de datos en el entorno de trabajo merece una regulación concreta en el Reglamento. El art. 88 RGPD se limita a realizar un llamamiento a los Estados miembros para que, a través de sus disposiciones legislativas o convenios colectivos, incluyan medidas específicas con el fin de preservar la privacidad de las personas trabajadoras con respecto al tratamiento y transferencia de los datos personales, en particular a efectos de la contratación, de la ejecución del contrato laboral[22] y de la extinción de la relación laboral. El tratamiento de los datos personales de las personas trabajadoras debe inspirarse en los principios generales declarados por el Reglamento europeo en su art. 5: licitud, lealtad y transpa-

[22] «Incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo», art. 88 RGPD.

rencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e integridad y confidencialidad.

2.3. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales

Siguiendo las instrucciones europeas se aprobó la Ley Orgánica 3/2018 de Protección de datos (en adelante LOPD) con el objeto de incorporar garantías adicionales que salvaguarden el derecho fundamental a la intimidad informática de las personas trabajadoras.

La protección de datos personales en el entorno laboral encuentra su regulación en el artículo 28 (obligaciones generales del responsable y encargado del tratamiento), en el artículo 87 (derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral), en el artículo 88 (derecho a la desconexión digital en el ámbito laboral), y en el artículo 89 (derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo).

El tratamiento de datos en la empresa y la adopción de medidas obliga al responsable a tener en cuenta los mayores riesgos que implica una evaluación de información personal con el objetivo de crear perfiles, mediante el análisis o la predicción de aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, el comportamiento, la localización o los movimientos.

Con el fin de proteger la intimidad de la persona trabajadora, el legislador regula el uso de dispositivos digitales facilitados por la empresa (art. 87 LOPD), permitiendo exclusivamente el acceso a la información a los efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y preservar la integridad del dispositivo. En aquellos supuestos en los que el dispositivo se utilice para fines privados, se deberán autorizar estos de forma específica. El tratamiento de los datos será adecuado cuando los trabajadores estén informados de los criterios empleados.

Es posible establecer otros dispositivos que permitan la videovigilancia, la grabación de sonidos y la geolocalización. Solo se permite la instalación de cámaras o videocámaras cuando su objetivo sea controlar la prestación de servicios de conformidad con lo previsto en el art. 20.3 de la Ley del Estatuto de los Trabajadores, siempre que los empleadores informen previamente, y de forma clara y expresa, a los trabajadores y representantes sobre la medida (art. 89 LOPD). La instalación de sistemas de grabación, tanto de imágenes como de sonidos, en lugares destinados al descanso o esparcimiento está prohibida legalmente. Solo se admitirá la grabación de sonidos en aquellos espacios que sean relevantes por los riesgos para la seguridad de las instalaciones, los bienes y las personas en relación con la actividad que se desarrolle en el centro y siempre que se atiendan los límites de proporcionalidad, intervención mínima y otras garantías ya comentadas (art. 89.3 LOPD). Por otro lado, el establecimiento lícito de sistemas de geolocalización dependerá de que el empleador informe previamente, de forma clara e inequívoca, a las personas trabajadoras y a sus representantes sobre los criterios de utilización de este dispositivo. Igualmente, deberá informar sobre los derechos de acceso, rectificación, limitación y supresión.

La protección específica del derecho a la desconexión digital es particularmente relevante en esta ley (art. 88 LOPD). Esta regulación no solo permite el ejercicio de otros derechos como la conciliación de la vida laboral, personal y familiar, sino que su efectividad permitirá una mayor protección de los datos personales, especialmente cuando la prestación de servicios esté vinculada con herramientas tecnológicas. En otros términos, garantizando una desconexión digital de la plantilla que trabaja en plataformas digitales, se compartirán menos datos personales y por ende se propiciará una mayor seguridad en la esfera privada de la persona.

A pesar de los avances normativos expuestos, tanto a nivel internacional como nacional, el régimen jurídico actual difícilmente puede proteger con efectividad el derecho a la intimidad informática en la empresa. Constantemente, aparecen nuevas lagunas jurídicas inherentes a un mercado de trabajo versátil y favorecido por el avance fugaz de la inteligencia artificial. Por este motivo, el legislador debe realizar un llamamiento directo a los agentes sociales con el fin de elaborar acuerdos de naturaleza sectorial que, entre otras cuestiones, especifiquen cuáles son los datos personales de las personas trabajadoras que pueden ser objeto de tratamiento por parte de la empresa y con qué finalidad.

3. LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA EMPRESA

3.1. Competencias y garantías

La norma suprema del ordenamiento jurídico español obliga a limitar por ley el uso de la informática para preservar diversos derechos fundamentales de las personas trabajadoras. Con el objetivo de cumplir con el mandato constitucional, surge la necesidad de nombrar en la empresa a un profesional que vele por el control de los datos almacenados. En este sentido, el delegado de protección de datos (*Data protection officer*) –DPD, en adelante– es una figura de creación legal que ejerce una función de naturaleza constitucional.

De conformidad con el art. 37 RGPD, cuando el responsable o encargado de los datos en una organización realice, entre sus actividades principales o primarias (no auxiliares), operaciones de tratamiento que requieran de una observación habitual y sistemática de la información, este tiene la obligación de nombrar a un delegado para la protección de los datos[23]. En todo caso, el art. 34 LOPD recoge

[23] La figura del DPD no es novedosa, pues su actividad se encontraba regulada en el derogado Reglamento (CE) n.º 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Especial mención realiza el considerando 24 del citado reglamento, al exponer lo siguiente: «Deberán adoptarse las medidas técnicas necesarias para permitir el acceso a los registros de los tratamientos efectuados por los delegados de la protección de datos a través de la autoridad de control independiente».

un listado de entidades que se encuentran expresamente obligadas a nombrar a un DPD, destacando, entre otras[24], las plataformas digitales por prestar servicios de comunicaciones electrónicas y manipular datos a gran escala.

El delegado de protección de datos puede ser una persona trabajadora de la empresa y formar parte de su plantilla o bien puede ser un tercero que desempeña su actividad en el marco de un contrato de servicios. Con independencia del vínculo contractual, el DPD es aquella «persona que, en el seno de un responsable o un encargado del tratamiento, supervisa y monitorea de forma independiente la aplicación interna y el respeto de las normas sobre protección de datos»[25]. Para su elección, es indispensable que el delegado o delegada cuente con las cualidades profesionales necesarias y, en particular, con los conocimientos especializados del Derecho y la práctica en materia de protección de datos, así como con la capacidad para desempeñar de forma exclusiva las competencias previstas en la normativa vigente[26]. Esta figura no debe confundirse con el responsable de seguridad, pues se trata de un profesional que es nombrado por acreditar sus conocimientos especializados y para ejercer exclusivamente sus funciones[27].

El delegado de protección de datos tendrá, como mínimo, las siguientes competencias previstas en el art. 39 RGPD: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento; b) supervisar el cumplimiento de lo dispuesto en la normativa comunitaria y nacional en materia de protección de datos personales; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación; d) cooperar con la autoridad de control; y e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Con el fin de proteger las enumeradas competencias, la normativa europea (art. 38.3 RGPD) y especialmente la estatal (art. 36 LOPD) reconocen la garantía de indemnidad del delegado, al no poder ser removido ni sancionado por desempeñar sus actividades, salvo que incurriera en dolo o negligencia. Para ello, es imprescindible reconocer el principio de independencia funcional que inspira la actuación de este profesional dentro de la organización, el cual sólo rendirá cuentas al más alto nivel jerárquico. Asimismo, en el desarrollo de sus funciones, el delegado de pro-

[24] Como los establecimientos financieros de crédito; las entidades aseguradoras y reaseguradoras; los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes; etc. En definitiva, están obligadas a nombrar un delegado de protección de datos todas aquellas empresas enumeradas en el art. 34.1 LOPD.

[25] Véase Comisión Europea, Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final, de 25 de enero de 2012.

[26] Debido a que la normativa europea exige una formación específica para ser designado como DPO, la Agencia Española de Protección, en colaboración con la Entidad Nacional de Acreditación y un Comité Técnico de Expertos, ha elaborado un sistema de certificación para ofrecer una mayor seguridad a los profesionales en la materia y las entidades que incorporen esta figura en su plantilla.

[27] Sierra Benítez, E.M., «El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico», *Revista Internacional y Comparada de Relaciones Laborales y derecho del empleo*, n.º 1, 2018, p. 244 y ss.

tección de datos está sujeto al deber de sigilo, manteniendo en secreto y de forma confidencial toda información que recoge en el desempeño de su cargo.

3.2. El alcance de la protección jurídica del delegado de protección de datos: la STJUE de 22 de junio de 2022, *Leistritz AG* contra *LH,* asunto C-534/20

La STJUE (Sala Primera) de 22 de junio de 2022, *Leistritz AG* contra *LH*, asunto C-534/20, resuelve la cuestión prejudicial planteada por el Tribunal Supremo Laboral de Alemania (*Bundesarbeitsgericht*). Atendiendo a la normativa alemana, las empresas están obligadas a designar un delegado/a de protección de datos. La trabajadora de la empresa, que responde a las siglas LH, prestó servicios en la empresa como directora del servicio de asuntos jurídicos, a partir del 15 de enero de 2018; y como delegada de protección de datos, a partir del 1 de febrero de 2018. El día 13 de julio de 2018, LH recibió un escrito de la empresa que declaraba la rescisión del contrato de trabajo por cuestiones de reestructuración empresarial al externalizar ambas actividades, tanto el servicio de asesoramiento jurídico como el servicio de protección de datos.

La trabajadora impugnó judicialmente el despido, aconteciendo que al propio órgano jurisdiccional se le presentó un conflicto en el que no existía doctrina pacífica. Por un lado, la opinión doctrinal mayoritaria consideraba que la protección especial contra el despido de la trabajadora prevista en la Ley alemana constituye una normativa material de Derecho laboral, respecto de la cual la Unión carece de competencia legislativa. Por otro lado, la opinión minoritaria defendía que los vínculos entre la protección y la función del delegado de protección de datos entran en conflicto con el Derecho de la Unión Europea.

Ante esta situación, el *Bundesarbeitsgericht* suspendió el procedimiento, para plantear la correspondiente cuestión prejudicial al Tribunal de Justicia de la Unión Europea sobre el alcance del art. 38 del 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. El apartado tercero del art. 38 del citado Reglamento general de protección de datos dispone lo siguiente:

> El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

La referida cuestión prejudicial versa sobre la interpretación y el alcance del art. 38.3 RGPD, a fin de evitar que la normativa nacional entre en contradicción con el Derecho de la Unión. En concreto, el Alto Tribunal pregunta si el artículo mencionado se opone a una ley estatal que permita despedir a un delegado de pro-

tección de datos por causa grave, aun cuando el despido no esté relacionado con el ejercicio de sus funciones. Para resolver esta cuestión, el Tribunal de Justicia manifestó diversas consideraciones, destacando por su trascendencia las siguientes.

En primer lugar, el art. 38 RGPD protege al delegado de protección de datos contra cualquier decisión que ponga fin a sus funciones, le sea desfavorable o constituya una sanción. Por su parte, el Reglamento (UE) 2016/679 trata de preservar la independencia funcional del delegado de protección de datos, así como garantizar la efectividad de las disposiciones previstas. En este sentido, el Considerando núm. 97 del Reglamento afirma que «tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente». Pues bien, una de las principales características de la implantación de un DPD en la empresa es la creación de un nuevo puesto con las siguientes peculiaridades: 1) autonomía en el ejercicio de la actividad; 2) relación directa con el nivel superior de la organización; y 3) obligación del responsable o encargado de facilitar al DPO todos los recursos necesarios para el ejercicio de sus funciones[28].

En segundo lugar, de conformidad con el apartado segundo del art. 153 TFUE, el Parlamento y el Consejo pueden adoptar disposiciones mínimas mediante directivas europeas, no pudiendo el TJUE impedir a los Estados miembros que mantengan o introduzcan medidas de protección más estrictas que las previstas en los Tratados. En palabras de la STJUE de 19 de noviembre de 2019, *Terveys-ja sosiaalialan neuvottelujärjestö* (TSN) *ry y Hyvinvointialan liitto ry*, asuntos acumulados C-609/17 y C-610/17, «los Estados miembros conservan la facultad, en ejercicio de la competencia que mantienen, de adoptar tales normas, más rigurosas que las que son objeto de la intervención del legislador de la Unión, siempre que no afecten negativamente a la coherencia de tal intervención». Lo que quiere decir que cada Estado tiene libertad para aprobar una normativa nacional específica en materia de protección de datos, siempre que la misma sea compatible con el Derecho de la Unión Europea y en particular con las disposiciones citadas del RGPD. Ahora bien, la protección reforzada que puede garantizar un Estado no es absoluta y tiene como límite no poner en peligro la consecución de los objetivos previstos en el Reglamento.

Para finalizar, en virtud de todo lo expuesto, el TJUE resuelve la cuestión prejudicial al declarar que el referido apartado tercero del art. 38.3 del Reglamento europeo de Protección de datos

> no se opone a una normativa nacional que establece que un responsable o un encargado del tratamiento solo puede despedir a un delegado de protección de datos que forme parte de su plantilla por causa grave, aun cuando el despido no esté relacionado con el ejercicio de las funciones de dicho delegado, siempre que esa normativa no ponga en peligro la consecución de los objetivos de ese Reglamento.

---

[28] Sierra Benítez, E.M., «El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico», *Revista Internacional y Comparada de Relaciones Laborales y derecho del empleo*, n.º 1, 2018, p. 256.

4. A MODO DE CONCLUSIÓN

El auge de las *Big Tech* ha propiciado la creación de un nuevo modelo productivo que radica en la extracción y sistematización de datos. Las compañías más exitosas son aquellas que tienen un mayor número de trabajadores digitales, pues el éxito empresarial responde a una doble prestación por la parte más débil del contrato de trabajo: en primer lugar, la realización de una obra o servicio por cuenta ajena; en segundo lugar, la transmisión inconsciente de información privada que incrementa los ingresos económicos de las compañías.

La digitalización de las relaciones laborales, impulsada por el capitalismo de datos o de la vigilancia, colisiona con la protección de determinados derechos fundamentales. El recurso a las nuevas tecnologías, y especialmente la aplicación de sistemas algorítmicos, propicia un nuevo conflicto ente la libertad de empresa y el derecho a la privacidad en el marco de la era digital.

Las personas trabajadoras tienen derecho a preservar su intimidad ante las nuevas facultades de dirección y control empresarial favorecidas por las innovaciones tecnológicas. Ante este escenario, surge el derecho a la intimidad informática como un derecho fundamental de tercera generación, autónomo e independiente que responde a las nuevas amenazas, retos y desafíos.

A pesar de los avances normativos, tanto a nivel europeo (Reglamento general de protección de datos) como a nivel nacional (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales), el régimen jurídico actual difícilmente puede proteger con efectividad el derecho a la intimidad informática de las personas trabajadoras en la empresa. Constantemente, aparecen nuevas lagunas inherentes a un mercado de trabajo versátil y favorecido por el avance fugaz de la inteligencia artificial. Por este motivo, el legislador debe realizar un llamamiento directo a los agentes sociales con el fin de elaborar acuerdos que aborden esta materia a nivel sectorial.

Por último, es imprescindible la protección de la figura del delegado/a de protección de datos en las organizaciones, pues este profesional acreditado tiene como función garantizar la aplicación interna y el respeto de la normativa vigente en la materia.

Recibido: 28/11/2022; aceptado: 23/01/2023