

BIG DATA: GESTIÓN DE RECURSOS HUMANOS Y EL DERECHO DE INFORMACIÓN DE LOS REPRESENTANTES DE LOS TRABAJADORES

BIG DATA: HUMAN RESOURCES MANAGEMENT AND THE RIGHT TO INFORMATION OF WORKERS' REPRESENTATIVES

FRANCISCA BERNAL SANTAMARÍA
Profesora Contratada Doctorada (acreditada)
Universidad de Cádiz
ORCID ID: 0000-0002-6744-3290

Recibido: 16.06.2020 / Aceptado: 03.07.2020

DOI: <https://doi.org/https://doi.org/10.20318/cdt.2020.5605>

Resumen: Se expone los retos que plantea la Era Digital, y de forma concreta, la “Era de los Datos” junto a la afectación a derechos fundamentales, como es el de derecho a la protección de datos de candidatas y de trabajadores. En este reto se analiza el Reglamento 2016/679 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 su proyección en las relaciones laborales. A su vez, se plantea la necesidad de que el algoritmo que genera el volumen de datos a disposición de las empresas sea conocido por los representantes de los trabajadores como parte integrante de sus derechos de información.

Palabras clave: big data, algoritmos, derechos de información, protección de datos, reglamento.

Abstract: In this article the challenges by the Digital Age are exposed, and specifically, the “Data Age” together with the affectation of fundamental rights, such as the right to data protection of candidates and workers. This challenge analyses Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of this data and its projection in labour relations. Therefore, the algorithm that generates the volume of data available to companies must be known by workers' representatives as an integral part of their information rights.

Keywords: big data, algorithms, information rights, data protection, worker's representatives, regulation.

Sumario: I. Introducción: algunas consideraciones en la delimitación del objeto de estudio. II. La tecnología como instrumento al servicio de las empresas: la gestión de los datos personales. 1. El papel del *Big Data* en la toma de decisiones empresariales: la creación de perfiles de candidatas-trabajadores. 2. La irrupción de la tecnología en los derechos de los ciudadanos-trabajadores. III. La afectación de la normativa internacional sobre la protección de datos a las relaciones laborales. IV. Estudio de la norma estatutaria y su necesaria reflexión a la luz del Reglamento y de la Ley Orgánica de Protección de Datos. 1. El rol de los representantes de los trabajadores en la Era Digital. 2. La autonomía colectiva en la Era Digital. 3. Los derechos de información y consulta en la Era Digital: el traslado de la funcionalidad del derecho de información como refuerzo del deber de secreto y de sigilo profesional. V. Conclusiones y propuestas de mejora.

I. Introducción: algunas consideraciones en la delimitación del objeto de estudio

1. En este análisis se abordan los problemas que proyecta la tecnología en la concreción del derecho de información de los representantes de los trabajadores. En concreto, el desarrollo de nanotecnología, el internet de las cosas, la red de redes, la inteligencia artificial, la tecnología portátil, la videovigilancia, la realidad aumentada, los wearables y de otros instrumentos. Dados los innumerables beneficios que aportan estos dispositivos, cada vez son más empresas las que optan por incorporarlos en la gestión de los recursos humanos. No obstante, esta Cuarta Revolución trae una serie de interrogantes de diferente ropaje. No cabe duda que el uso de la tecnología por parte de la empresa incrementa exponencialmente la disponibilidad de datos personales y profesionales (lo que se conoce como *Big Data*). Y, a su vez, amplía las posibilidades de control y vigilancia de la empresa desde la etapa precontractual a la finalización o extinción del contrato de trabajo.

2. En efecto, en la Era Digital, el uso de algoritmos conduce a la creación de perfiles como una información complementaria que tiene la empresa para la gestión del personal (desde el acceso al empleo, la clasificación profesional, la promoción e incluso el ejercicio del poder de dirección y del poder disciplinario sancionador).

En el seno de estos poderes, nos planteamos diferentes cuestiones relacionadas con la actividad de los representantes de los trabajadores en su relación con la protección de datos, y de forma concreta, el grado de responsabilidad en cuanto al deber de secreto y de sigilo profesional que se les podría imponer. Este aspecto es de importancia en lo que afecta a los derechos estipulados en el artículo 4.1 g) (derecho de información, consulta y participación), así como en el artículo 4.2. e) (derecho al respecto a su intimidad) del Estatuto de los Trabajadores¹.

3. En esta sede de análisis, se trata de abordar cómo la tecnología altera instituciones clásicas como el deber de sigilo y de secreto profesional, con la aparición de figuras que representan concretos derechos de los trabajadores, como son los datos personales de estos de los que dispone la empresa.

4. En esta aportación se concebirá una lectura positiva del progreso de la tecnología para proteger los derechos de los trabajadores en la que se repensarán las funciones y se reservarán concretas funciones para los representantes de los trabajadores².

5. La regulación de los derechos de información y consulta, así como la protección de los datos personales justifica una metodología clásica. Por tanto, para el planteamiento de este problema se investigarán los preceptos de la norma estatutaria que tratan de forma tradicional el mismo, y se acudirá a la normativa internacional aplicable en España.

6. De forma específica, se recurrirá a instancias supranacionales para analizar principalmente al Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos³. Junto a ello, al marco normativo español que incorpora

¹ Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255 de 24 de octubre de 2015).

² De referencia en esta materia es E. GARRIDO PÉREZ, “Los cambios sistemáticos, materiales y funcionales en los derechos de información y consulta de los representantes de los trabajadores del personal”, *Temas laborales*, núm. 95, 2008, pp. 11- 44; “La impronta del Tribunal de Justicia de la Unión Europea en el tratamiento español de los derechos de información y consulta” *Temas Laborales*, núm. 130, 2015, pp. 351-393.

³ 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 (Reglamento general de protección de datos- RGPD). DOUEL núm. 119 de 04 de mayo de 2016. Cabe poner de manifiesto que este Reglamento deroga la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de datos de personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de esos datos. Esta derogación obedece, entre otros motivos, a la vertiginosa irrupción de los cambios tecnológicos en esta Cuarta Revolución. Otro objetivo importante del Reglamento es la uniformidad pretendida de cara a conformar una aplicación homogénea y uniforme, a la par que sea directamente aplicable a los Estados.

esta normativa, a la doctrina que ha venido estudiando estas consideraciones y, también, a la actuación de los interlocutores sociales en esta materia.

7. Con estos cimientos, se extraerán una serie de conclusiones propias y relevantes para tratar de avanzar en el enriquecimiento jurídico aplicable al problema planteado. Tras este análisis del estado de la cuestión se tratará de aportar conclusiones con propuestas de *lege ferenda* para concretar unas reglas vinculantes al caso que se ha planteado.

II. La tecnología como instrumento al servicio de las empresas: la gestión de los datos personales

8. La sociedad digital actual se erige sobre cimientos creados por el ser humano, como nuevas técnicas, dispositivos, aparatos y descubrimientos que han dibujado un mundo que nos ofrece retos y oportunidades, pero también inquietantes riesgos para los derechos y libertades fundamentales, para la democracia y para la economía de mercado⁴.

9. En la Era Digital es un objetivo prioritario de las empresas la recopilación y tratamiento de aquella información que le permita una toma de decisiones lo más óptima y eficiente posible. Con ello, la gestión de toda esta información es un cambio radical para los modelos de negocio y para el departamento de los recursos humanos de las empresas. Lo que no ha cambiado es que en el mundo laboral sigue reinando una realidad y es que el objetivo prioritario de las empresas es la maximización del beneficio. Un objetivo compartido por la tecnología, pues “la maximización del beneficio empresarial es la razón de ser última de toda innovación tecnológica”⁵.

10. Dicho esto, es lícito que las empresas deseen tener información sobre sus trabajadores, en la medida en que ello repercuta en su productividad y aumento de beneficios. Así, queda dentro de la potestad de vigilancia y control, que el empresario obtenga información en relación a cuestiones como el nivel de productividad, la capacidad de adaptación a la política de la empresa, o las habilidades, aptitudes y actitudes en el desempeño de su puesto de trabajo.

11. Ahora bien, una cosa es que las empresas gestionen datos relacionados con estos aspectos, y otra bien distinta es que gestionen datos personales conectados con su privacidad y con su derecho a la intimidad. Es en este aspecto en el que se arbitra la protección de datos personales, que trata de instituir un “conjunto de técnicas llamadas a dar soporte y garantizar el ejercicio del derecho a la autodeterminación informativa, concebido como la capacidad y derecho de los individuos de ejercer el control sobre las informaciones que le atañen”. Este principio “se convierte en la defensa eficaz para la esfera privada del individuo frente al peligro de la informatización de los datos personales”. Así, este principio se erige como un instrumento para garantizar otros derechos como el de la intimidad, o el derecho al honor, a la dignidad y a la libertad de la persona, de manera que el sujeto afectado puede limitar y racionalizar la utilización y el tratamiento de sus datos personales⁶.

12. No cabe duda que la Era digital es una propulsión que genera cambios imprevisibles en la sociedad, en la economía y en el mercado laboral. Su imparable desarrollo ofrece grandes oportunidades y beneficios para las personas en general, pero también provoca ciertos recelos. Una preocupación im-

⁴ En esta línea léase a T. DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, “Retos, Riesgos y Oportunidades de la Sociedad digital”, En *Sociedad Digital y Derecho*, Boletín Oficial del Estado, Ministerio de Industria, Comercio y Turismo y RED.es, Madrid, 2018.

⁵ Cfr. M. R. ALARCÓN CARACUEL, “La informatización y las nuevas formas de trabajo”, En *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete 2004, p. 10.

⁶ M. B. CARDONA RUBERT, “Protección de Datos Personales”, En *Diccionario Internacional de Derecho del Trabajo y de la Seguridad Social*, Tirant Lo Blanch, Valencia, 2014, pp. 1809-1811.; Sobre la autodeterminación informativa C. MOLINA NAVARRETE, “Acción sindical y protección de datos: nuevos relatos de una relación espinosa”, *RTSS CE*, núm. 423, 2018, p. 142.

portante es su capacidad para tratar a gran velocidad los datos de las personas, adquiriendo “una dimensión esencial las manifestaciones de identidad subjetiva, esas huellas digitales que las personas dejan al contratar una tarjeta de crédito, dar de alta una wifi navegar por Internet, realizar una compra, etc. Esa cesión constante de datos comporta un riesgo para la privacidad, y plantea la necesidad de una efectiva tutela de la persona frente al tratamiento de sus datos”⁷.

1. El papel del *Big Data* en la toma de decisiones empresariales: la creación de perfiles de candidatos-trabajadores

13. Cualquiera de los dispositivos digitales y tecnológicos llevan instalados sensores, aplicaciones, lectores de identificación, cámaras o micrófonos, y comparten entre sí un fin “inquietante”: su capacidad para generar datos. Unos datos que pueden ser gestionados para obtener información relevante sobre los ciudadanos-trabajadores. Esta interacción y acumulación de datos hace posible recoger numerosos aspectos de la vida de la persona que usa ese tipo de dispositivos y de redes. Ello traza el aspecto fundamental de esta Revolución: el acelerado proceso de digitalización de datos con la utilización de algoritmos⁸.

14. En ese fin tiene un protagonismo absoluto el *Big Data*, definido como un instrumento con capacidad no solo para captar una gran cantidad y volumen de información (altamente heterogénea), sino también para gestionarla con algoritmos, la computación y la analítica. La gestión de esta información permite que sea accesible y utilizable para diferentes propósitos. Téngase en cuenta que los datos por sí solos no tienen sentido intrínseco, y solo lo tendrán cuando sean portadores de información y se retransmita a personas o máquinas, esto es, cuando sean objeto de comunicación. La digitalización tiene como fin el tratamiento de datos analógicos y su conversión en datos digitales. Así, los datos digitales generan un valor añadido, son un factor de producción más en la sociedad moderna y quedan dotados de gran relevancia económica⁹.

15. Con ello, la procedencia de los datos nace desde las transacciones y el uso de distintas webs y de redes sociales, datos que generan las personas o las máquinas. Se trata de interacciones como las búsquedas en Google, subida de fotos y clics en Facebook, subida de fotos en Instagram, viralización de Tweets o visualización de videos en YouTube o en otros sitios webs. Son millones de usuarios generando datos que se multiplican exponencialmente cada segundo desde dispositivos digitales (teléfonos, ordenadores, redes sociales, tarjetas de compras y tarjetas de puntos, el GPS y un sinfín de dispositivos de nueva creación, etc.).

16. Con este contexto, y con la fiebre por el uso de dispositivos, el auge de las redes sociales tanto profesionales como personales, y la transformación digital de las ciudades se multiplican exponencialmente los volúmenes de datos, pues cada segundo, todo tipo de sensores en tabletas, teléfonos, junto las redes sociales y las transacciones en plataformas como Amazon, AliExpress o Walapop, generan grandes cantidades de datos de los ciudadanos que revelan nuestros estados de ánimo y emociones, nuestros gustos, nuestras costumbres y nuestra forma y estilo de vida; incluso, delatan otros aspectos

⁷ Cfr. J. L. GOÑI SEÍN, “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016”, *Revista de derecho social*, núm. 78, 2017, pp. 15-42.

⁸ Uno de los principales (y más perversos) usos de la dictadura de los datos es la creación de perfiles de ciudadanos. La gestión automatizada de los datos de las personas permite trazar predicciones de comportamiento. El mayor riesgo es que este perfil (de los resultados obtenidos de los algoritmos formulados) se emplee a modo de sesgo que excluya a determinados sectores (minoritarios) y ello entrañe una decisión discriminatoria. Por sectores minoritarios entiéndase a grupos vulnerables, entre otros, las mujeres, la clase social, los inmigrantes y las personas con discapacidad.

⁹ Es reiterado recurrir a la metáfora al comparar *Big Data* con el petróleo crudo por su alto potencial y capacidad para generar riquezas. Aun más, se ha expuesto el mayor rendimiento del *Big Data* frente a la industria petrolífera, no solo por las reservas ilimitadas de datos y porque estas se vean acrecentadas sin o contra la voluntad de los afectados, sino por el aumento constante de los depósitos de datos en manos de operadores globales y poderosos como Google, Amazon o Facebook. W. HOFFMANN-RIEM, *Big Data. Desafíos también para el Derecho*, Thomson Reuters Aranzadi, Navarra, 2018, pp. 51-57.

relacionados con nuestra esfera más íntima, como nuestra salud, nuestros hábitos y preferencias, nuestra ideología, creencias o nuestra vida afectiva, sexual o amorosa. Todo ello, dibuja un perfil íntimo de la persona y puede terminar trazando un grupo de personas con un perfil similar¹⁰.

17. No cabe duda que la “hiperdatificación” y el manejo del *Big Data* puede afectar con especial virulencia en todos y cada uno de los aspectos de la relación de trabajo. Así es plausible que las empresas puedan hacer coincidir a los candidatos cualificados con oportunidades de empleo y alienando la educación y el desarrollo de habilidades con las necesidades de la economía.

18. Del modo dibujado, lo cierto es que la educación, la experiencia laboral y los intereses se conectan para compilar un perfil de calificaciones precisas que puede alinearse con las habilidades y experiencia que los empleadores necesitan. A medida que ello evolucione, esta capacidad mejorará la eficacia con la que se hace coincidir a los solicitantes de empleo con los puestos de trabajo.

19. Ahora bien, el peligro que comporta este tipo de fórmulas es que permite la transmisión de datos (combinación de los mismos) a través del uso de ficheros de datos, junto al peligro de la descontextualización de la información, lo que creará un clima psicosociológico de control y transparencia, esto es, la conciencia en los trabajadores de poder ser conocidos en todos sus aspectos. No se puede obviar que la tecnología ofrece la posibilidad de vigilar y controlar a los trabajadores en diferentes planos, tanto el profesional, como el personal, llevando al trabajador a un estado de visibilidad permanente¹¹.

20. En la misma línea, la tecnología, la posibilidad de analizar ingentes cantidades de datos, el aprendizaje automático y la inteligencia artificial, unida a la amplia disponibilidad de encontrar datos de las personas en internet, facilita la creación de perfiles y la automatización de decisiones empresariales que producen efectos jurídicos. Desde luego, de la creación de perfiles y de las decisiones automatizadas resulta un considerable ahorro de costes y una mayor eficiencia para las empresas. No obstante, también tienen un alto potencial de afectar de forma significativa a los derechos y a las libertades de las personas. En ello, se ha considerado la necesidad de unas garantías adecuadas para evitar este y otros riesgos paralelos como es principalmente la intimidad, pero también, la segregación social, los estereotipos discriminatorios, y la opacidad en la que ni los propios sujetos afectados sean conscientes de que se están creando perfiles de su personalidad¹².

21. En este orden de cosas, la protección de Datos personales (y la autodeterminación informativa) son los cimientos para que las personas se defiendan de un uso ilegítimo en el tratamiento de sus datos relacionados con la información personal. Se trata de aquellos aspectos personales o de la vida que de forma aislada no tienen relevancia, pero que convenientemente combinados y analizados de forma cruzada entre sí “arrojan como precipitado un retrato de la personalidad del individuo que éste tiene

¹⁰ Sobre las redes sociales y los derechos de los trabajadores vid. M. B. CARDONA RUBERT y C. CORDERO GORDILLO, “Redes Sociales y Derechos Colectivos”, *Revista Direito e Desenvolvimento, Joao Pessoa*, v.6, núm. 11, 2015, pp. 133-149.

¹¹ Sobre lo apuntado, un autor experto en la materia es J. R. MERCADER UGUINA, “El mercado de trabajo y el empleo en un mundo digital”, *Revista de Información Laboral*, núm. 11, 2018. Es muy interesante acudir una obra dedicada a los efectos de la Revolución tecnológica sobre el mercado de trabajo, especialmente, el impacto del control empresarial sobre los derechos de los trabajadores a la dignidad e intimidad, incluso con apuntes a los aspectos procesales como los de la prueba digital F. LOUSADA y R.P. LATAS, “Control de la actividad laboral a través de tecnologías de la información y la comunicación: la situación de España”; L. M. MUNÍN SÁNCHEZ, “La prueba laboral ante la digitalización del proceso”, L. MELLA SÁNCHEZ, “Sobre la prueba digital en el derecho español: puntos críticos”, en *La Revolución tecnológica y sus efectos en el mercado de trabajo: un reto del siglo XXI, Temas La Ley*, 2018; M.J. CERVILLA GARZÓN, “Efectos del uso de la aplicación “WhatsApp” en el marco de las relaciones laborales, *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 136, 2017, pp. 73-97.

¹² Vid. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. Toda la información de la labor y de las funciones en https://ec.europa.eu/justice/article-29/documentation/index_en.htm (Último acceso: 5 de marzo de 2020). Desde una perspectiva de la discriminación en base al género, léase E. M. SIERRA BENÍTEZ, “¿Las nuevas tecnologías influyen en la discriminación o la van a eliminar?”, *Noticias Cielo*, núm.10, 2019.

derecho a mantener reservado” y “permite al empresario reconstruir a partir de datos aparentemente inocuos, el perfil del trabajador, perfil de ser susceptible de ser utilizado con los fines más variados”. Ello se traslada al ámbito laboral con la intimidad informática-informativa del trabajador que alcanza a los aspectos de la vida privada que confiere al trabajador la potestad de conocer y controlar las transacciones y las operaciones (la gestión de sus datos personales) que realicen las empresas¹³.

22. En este mismo orden, y en relación al problema planteado, podemos enfrentar a ver como lo afronta la norma. Pues bien, el derecho a la protección de datos se refuerza en las disposiciones del RGPD cuando su artículo 15 dispone que el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información relacionada.

23. En este punto, conviene aclarar qué se entiende por tratamiento de datos, por elaboración de perfiles y por decisiones automatizadas que afecten a los trabajadores en el seno de las relaciones de trabajo.

24. El artículo 4.2 del RGPD define el tratamiento como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”. La definición aportada nace con una vocación de amplitud con el fin que cualquier operación que se haga con datos personales se considere tratamiento. Del modo relatado, el RGPD será aplicable a cualquier situación en la que se esté ante datos personales y éstos sean objeto de tratamiento automatizado (ya sea parcial o total).

25. Por su parte, es esencial analizar el artículo 22 del RGPD que se encarga de tutelar los intereses de las personas afectadas por la elaboración de perfiles y por las decisiones automatizadas. En este sentido, prevé que todo sujeto tiene el derecho a no ser objeto de una decisión únicamente basada en el tratamiento automatizado (incluida la elaboración de perfiles) cuando produzca efectos jurídicos sobre él o le afecte significativamente¹⁴. Ello incluye cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento futuro (dentro y fuera de la empresa), la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar¹⁵.

26. En este punto, el Grupo de Trabajo 29 interpreta que el “derecho a la protección de datos” no se aplica solo cuando el interesado lo invoque de forma activa, sino que esta prohibición se aplica tanto si el interesado adopta una acción sobre el tratamiento de sus datos, como si no lo hace¹⁶. En este

¹³ Cfr. M. B. CARDONA RUBERT, “Protección de Datos Personales...”, op. cit. p. 1810.

¹⁴ El RGPD dispone una serie de excepciones a la regla general de prohibición de decisiones automatizadas, si: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; o c) se basa en el consentimiento explícito del interesado. A su vez, prevé que si se aplica la excepción b) se deben establecer medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del afectado. Mientras que si se aplican algunas de las otras dos excepciones el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

¹⁵ Así se expone en el Considerando 71 de la Exposición de Motivos del RGPD.

¹⁶ El Grupo de Trabajo del artículo 29 es un grupo de trabajo europeo independiente que se creó con la Directiva 95/46/CE con funciones consultivas, de asesoramiento y contribución a la aplicación uniforme de las normas nacionales en relación a la protección de la privacidad y de los datos personales. Este Grupo se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (fecha de entrada en aplicación del RGPD), emitiendo

sentido, la interpretación dada por el Grupo de Trabajo refuerza que el sujeto tenga el control sobre sus datos cumpliéndose así uno de los principios fundamentales del Reglamento, y es que precisamente el derecho de la protección de datos incluye el control de los mismos frente a determinados tratamientos. Igualmente, el sujeto queda automáticamente protegido frente a las posibles consecuencias que pueda tener este tipo de tratamiento.

27. De la manera relatada y base en los argumentos aportados, se ha señalado que no es posible tomar decisiones automatizadas, ni basadas en perfiles creados automáticamente, en “materia de ascensos o concesión de bonus salariales y, menos, para despidos sin que exista intervención humana de carácter significativo”¹⁷. Conjuntamente, ello lleva a anotar que “se debe procurar que haya un ser humano con autonomía y control sobre las inteligencias artificial, un humano al mando”¹⁸. En este aspecto, se ha debatido sobre el alcance de la protección del Reglamento en este aspecto particular. En nuestra opinión, el Reglamento será aplicable siempre que se trate de decisiones automatizadas (sin intervención humana), y ante situaciones semi-automatizadas (la intervención humana se limita a ejecutar el resultado dado por el algoritmo). Pero también alcanza a aquellas situaciones en las que la decisión se toma con intervención humana (más o menos significativa), pero que ha sido basada en datos automatizados, es decir, una decisión fundamentada en los datos que ha aportado el algoritmo¹⁹.

28. De hecho, el RGPD define la “elaboración de perfiles” como “toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física” (artículo 4.4). En efecto, se aclara que “la elaboración de perfiles debe implicar cierta forma de tratamiento automatizado, aunque la participación humana no excluye necesariamente la actividad de la definición”.

De este modo, el recurso de algoritmo se podría concebir como una herramienta que facilita la toma de decisiones, pero una decisión que sigue estando en manos del responsable de recursos humanos. En modo alguno nos postulamos en que el *Big Data* sea una herramienta para eliminar la posibilidad de control y de decisión humana, de tal manera que termine por sustituir al director o responsable de los recursos humanos. Claro que, para evitar esta futura sustitución, se deben arbitrar medidas destinadas a tal fin (que sean fruto de la heteronomía y de la autonomía colectiva).

29. El propio RGPD así lo prevé cuando señala que “A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto”²⁰. Desde luego, es esencial contar con instrumentos y formación adecuada para dotar a los modelos algorítmicos de la suficiente eficacia y precisión para que determinen un resultado legal, legítimo y respetuoso con la normativa vigente.

decisiones en forma de Dictámenes o Informes.

¹⁷ Cfr. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos en las relaciones laborales: “big data”, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos”, *Revista de derecho social*, núm. 84, 2018, p. 76.

¹⁸ *Ibidem*.

¹⁹ *Ibidem*.

²⁰ En este sentido, téngase en cuenta que las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas. Vid. Considerando 71 del RGPD.

2. La irrupción de la tecnología en los derechos de los ciudadanos-trabajadores

30. Los cambios tecnológicos sucedidos han incidido de forma intensa en el recurso de herramientas empresariales para controlar de forma continua la actividad o la prestación laboral debida de sus trabajadores. Esta dimensión de las relaciones laborales ha sido catalogada como empresa panóptica en la que los instrumentos de control y seguimiento a disposición del empresario ofrecen detallada información sobre la prestación laboral de los trabajadores²¹.

31. Junto a ello, se ha dibujado un marco pivotado sobre dos ejes, uno en el que el ciudadano-trabajador interacciona continuamente con su entorno, siendo o no consciente de ello, como si fuera un diálogo interactivo continuo; y otro eje en el que las personas se han despojado de todo ropaje y se han convertido en ciudadanos de cristal, totalmente transparentes, conviviendo en una sociedad panóptica en la que todos los aspectos de las personas son conocidos²².

32. En esta era de la ubicuidad tecnológica, también llamada tecnología disruptiva fruto de la confluencia de la globalización y de la tecnología, se han trazado nuevos retos en el mercado de trabajo²³. Hoy día es posible que las empresas utilicen dispositivos para controlar y, en su caso, sancionar a las personas trabajadoras. Estamos hablando desde tarjetas de identificación (con reconocimiento facial y de las figuras de trabajadores), sistemas informatizados de las puntuaciones realizadas por los clientes a trabajadores, micrófonos que valoran los estados de ánimo de éstos y cómo ello repercute en su productividad, o monitores que miden de forma inmediata su aptitud y su prestación laboral.

33. Nuevamente, este tipo de dispositivos generan una información incalculable (por su alto valor añadido) y muy barata en atención a los beneficios que conlleva. Así, se puede presentar una situación en la que un trabajador sea advertido, sancionado y luego sea despedido a razón de la categorización de la información realizada por el algoritmo. De la misma forma, la interacción de los ciudadanos y el uso de la tecnología antes referida produce una ingeniería de datos que son proporcionados en muchos casos sin percepción ni intervención humana. De esta manera, cuando un trabajador equipado con dispositivos inteligentes está en la oficina o en la fábrica, o se desplaza en el vehículo de la empresa para la ejecución de la prestación debida, está enviando constantemente datos a la empresa sobre su actividad, su disposición geográfica y su interacción con los clientes. En este marco, cabe mencionar los ejemplos del uso de dispositivos o redes de internet en el seno de las empresas como son el *roaming*, la conexión a la red *wifi*, o la pulsera o una cámara que esté registrando la actividad de los trabajadores en el ejercicio de su prestación laboral²⁴.

²¹ Sobre la empresa panóptica es oportuno acudir a la extensa obra de J.R. MERCADER UGUINA, *Protección de datos y garantías de los derechos digitales en las relaciones laborales*, Francis Lefebvre Madrid, 2018, p. 29; “Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?”, *Relaciones laborales: Revista crítica de teoría y práctica*, núm. 1, 2001, pp. 665-686; “Les libertés individuelles dans l’entreprise à l’épreuve des nouvelles technologies. Observations à partir de la situation espagnole”, *Les libertés individuelles et relations de travail : le possible, le permis et l’interdit?* Presses Universitaires de Bordeaux, 2011.

²² Es muy ilustrativo el trabajo de C. SÁNCHEZ-RODAS NAVARRO, “Poderes directivos y nuevas tecnologías”, *Temas Laborales*, núm 138, 2017, pp. 163-184; J.R. MERCADER UGUINA, *Protección de datos y garantías de los derechos digitales en las relaciones laborales*, op. cit., p.78; Con un plano optimista M. C. AGUILAR GONZÁLVIZ, “Digitalización o la oportunidad de creación de más y mejores empleos”, *Estudios financieros. Revista de trabajo y seguridad social: Comentarios, casos PRÁCTICOS: recursos humanos*, núm. 445, 2020, pp.93-120; C. JÓVER RAMÍREZ, “Nuevas tecnologías, nuevas formas de empleo y nuevos ámbitos de redireccionamiento”, en J. M. GÓMEZ MUÑOZ (dir.), *El trabajo autónomo en España tras la crisis. Perspectivas y propuestas*, 2019, pp. 239-272.

²³ La doctrina ha señalado que el cambio tecnológico ha dibujado un nuevo escenario anunciando una nueva forma de entender el mercado del trabajo y el empleo en el mundo digital, redundando en una verdadera disrupción o destrucción creativa con un proceso permanente de innovación característica de la maquinaria del capitalismo J.R. MERCADER UGUINA, “El mercado de trabajo y el empleo en el mundo digital”, *Revista de Información Laboral*, núm. 11, 2018; S. RODRÍGUEZ ESCANCIANO, “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Estudios financieros. Revista de trabajo y seguridad social: Comentarios, casos prácticos: recursos humanos*, núm. 423, 2018, pp. 19-62.

²⁴ Sobre ello existen diferentes trabajos publicados, entre otros, S. DEL REY GUANTER, *Proyecto Technos. Internet of things y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales*, Wolters Kluwer. Madrid, 2017, p. 37.

34. Las empresas son muy conscientes de esta realidad y son cada vez más las que recurren a un buen manejo del *Big Data* para la toma de decisiones sobre la política de selección de la empresa y sobre la gestión de sus recursos humanos en el seno de la misma. Una toma de decisiones que permite a los gestores de los recursos humanos “predecir escenarios futuros y anticiparse, que podrán saber “qué hará un empleado (comportamiento), qué conseguirá (rendimiento) y cómo estará (satisfacción)”²⁵”.

Conjuntamente, la digitalización masiva de los datos comporta una serie de riesgos para los ciudadanos general, y para los trabajadores en particular. Así, podría quedar afectada la propia libertad individual, las condiciones de vida y de trabajo en la que se desarrolla la actividad humana, los derechos fundamentales del ciudadano-trabajador, la protección frente a la discriminación y a la propia observancia de los principios más básicos recogidos en el Estado de Derecho.

35. En este orden de ideas, la empresa debe tener especial cuidado a la hora de diseñar el algoritmo para que no albergue ningún sesgo discriminatorio. Téngase en cuenta que la tecnología tiene la capacidad de recabar información personal, aunque se prohíba considerarla (religión, discapacidad, ideología, etc.)²⁶. Es decir, habida cuenta que el algoritmo se nutre de datos estadísticos, se puede dar la posibilidad que prediga datos íntimos de las personas, como son su ideología, su religión o su clase social.

36. En síntesis, si tenemos en cuenta que “la propia construcción del algoritmo requiere de datos que están sesgados por parámetros discriminativos “y que “cuando un algoritmo está al mando, en general, las minorías siempre están en desventaja” nos lleva a que “el procesamiento automatizado de datos incrementa exponencialmente las posibilidades de vulneración de los derechos de los trabajadores”²⁷.

III. La afectación de la normativa internacional sobre la protección de datos a las relaciones laborales

37. Como declara la propia Exposición de Motivos del RGPD, “una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad”. De modo que los poderes públicos deben generar políticas legislativas que promuevan la igualdad y el pleno ejercicio de los derechos fundamentales en esta Era Digital. A pesar de reconocer el carácter innovador de nuestra Constitución al adelantarse a la protección del derecho a la intimidad (y de los derechos fundamentales) ante el impacto de la tecnología, lo cierto es que se demanda que la Constitución recoja los derechos fundamentales en la sociedad digital, de modo que eleve a rango constitucional una nueva generación de derechos digitales²⁸.

38. Llegados a este punto, es el momento de conocer el impulso del legislador europeo (y nacional) en la materia para tutelar a las relaciones laborales en la Era Digital.

La UE ha propulsado un conjunto normativo delimitador de la materia que ha tratado de garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, de forma

²⁵ Cfr. L. TABURET, La capacidad de predecir y comprender comportamientos humanos con Big Data <https://www.linkedin.com/pulse/la-capacidad-de-predecir-y-comprender-comportamientos-laura-taburet> (Último acceso: 10 de marzo de 2020). Sobre la selección de trabajadores es IMPRESCINDIBLE J. CRUZ VILLALÓN, *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites de la actuación del empleador*, Bomarzo, Albacete 2019; O. GARCÍA COCA, *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, Laborum, 2016.

²⁶ El artículo 9 del RGPD prohíbe el tratamiento de 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 la orientación sexual de una persona física.

²⁷ Cfr. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos ...”, op.cit., p. 74.

²⁸ Vid. Preámbulo IV de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294 de 6 de diciembre).

particular, del derecho a la vida privada, en lo que respecta al tratamiento automatizado de los datos personales²⁹.

39. En este impulso destaca el RGPD que responde a “los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información”. Su propia Exposición de Motivos aprecia el carácter central de los datos personales y considera los aspectos positivos de ésta, pero también los riesgos, principalmente, el riesgo de que la información sea más accesible por mas actores, que sea más fácil de procesar, mientras que sea hace más complicado el control de su destino y de su uso.

Para ello, el Reglamento dispone revisar las bases legales del modelo europeo de protección de datos en aras de reforzar la seguridad jurídica y la transparencia. En este sentido, el legislador español adoptó una nueva norma para adaptar el ordenamiento español a esta disposición europea persiguiendo el principio de seguridad jurídica, la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD)³⁰.

40. La LOPD establece el derecho fundamental de las personas físicas a la protección de datos personales. A su vez, trata de garantizar los derechos digitales de los ciudadanos conforme al artículo 18.4 de la Constitución Española (secreto de las comunicaciones), junto con el derecho a la intimidad personal y familiar enunciada en el artículo 18.1 de Carta Magna.

41. Pues bien, considerando que la tecnología afecta intensamente a estos intereses jurídicos protegidos como derechos fundamentales de la persona, se ha generado un contexto que tambalea los cimientos del Derecho a la intimidad. Se han destacado tres elementos importantes en este derrumbe. El primero es que el derecho a la intimidad queda limitado por la potestad de control empresarial. Es sabido que el derecho a la intimidad es un bien sacrificable y modulable para que el empresario pueda verificar el cumplimiento de la actividad. A su vez, la tecnología ha modulado este bien jurídico, pues la permanente interconexión virtual va reduciendo cada vez más el espacio y la esfera más íntima de la persona. El último elemento es el nuevo paradigma de internet que obliga a revelar datos personales como requisito de acceso a las redes sociales, o a aceptar las cookies para seguir navegando por la red. Todo ello genera una nueva forma de relacionarse, una necesidad de conectividad que derriba los muros individuales y crea una inteligencia colectiva que resulta accesible para muchas personas.

42. En este panorama, “la sociedad de la información ha provocado un cambio en la concepción de la intimidad y obliga a pensar y defender lo privado de manera diferente”³¹. En esta línea, la sociedad está enfocada en el control de la identidad de la persona, que no pierda el control de los datos personales, de la información que se recoge, cómo se trata, con qué fines se utiliza y decidir en consecuencia con el propósito de impedir su tráfico ilícito y lesivo de su derecho a la dignidad. La doctrina continúa señalando que la evolución de la tecnología y su capacidad para recolectar información es imparable. Por tanto, la defensa del interés legítimo del trabajador es controlar su identidad propia conforme al principio proclamado por el RGPD y por la LOPD. De esta forma, podrá ejercer un control sobre posibles usos indebidos para evitar las discriminaciones o exclusiones en el acceso al empleo o durante la relación laboral³².

43. En este punto, es importante subrayar que la protección de datos personales ha sido considerada como un derecho autónomo e independiente que se configura como un derecho fundamental

²⁹ Artículo 1 del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (BOE núm. 274, de 15 de noviembre de 1985). En el mismo sentido, se pronunciaba la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

³⁰ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294 de 6 de diciembre).

³¹ Cfr. J. L. GOÑI SEIN, “Nuevas tecnologías digitales ...”, op. cit. pp. 7 y 8.

³² *Ibidem*.

con base en los conceptos de intimidad y privacidad protegidos en el artículo 18 de la CE³³. Para garantizarlo se aboga porque la persona afectada tenga el control sobre sus datos personales, sobre su uso y su destino, que tenga un poder de disposición y control. Es decir, que la persona pueda decidir qué datos da a un tercero, o que datos puede recabar ese tercero, incluso que la persona pueda saber qué datos tiene ese tercero, y para qué puede estar utilizando, incluso pudiéndose oponer a esa posesión o uso. Con ello, se pueda evitar el tráfico ilícito de sus datos, que le sean lesivos para su dignidad y para afectación de sus derechos.

44. En síntesis, se le reconoce la potestad al ciudadano para oponerse a que sus datos personales sean usados para fines distintos a aquel que justificó su obtención³⁴. El principal problema es que la información recogida del trabajador sea utilizada para una finalidad distinta de la que justifica su recopilación, su gestión y tratamiento, hasta el punto que pueda ser tachada de discriminatoria si los datos transformados en conocimiento llegan a tener un resultado en sí mismo inaceptable. Un ejemplo ilustrativo es “si determinan la preferencia de un determinado sexo frente al otro, o el rechazo de determinadas personas con algunos componentes hereditarios o genéticos o con propensión a enfermar”³⁵.

45. En otro orden de cosas, sucede que la LOPD conjuga varios principios que ordenan la tutela del derecho a la identidad. El principio de transparencia se concreta en que los afectados deben ser informados acerca del tratamiento y recoge la denominada información por capas ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (Título III de la LOPD). Otro principio es el de responsabilidad activa que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan (Título V de la LOPD).

46. Por su parte, el principio de confidencialidad enunciado en el artículo 5, en términos de secreto profesional, es un deber de los responsables y los encargados del tratamiento, así como de cualquier persona que intervenga en cualquier fase sujeta al deber de confidencialidad. Por último, es importante destacar el principio de consentimiento recogido en el artículo 6 como toda manifestación (del afectado) de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Este principio (el de confidencialidad) es matizado al entender que no puede 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. Ello no quiere decir que en el contrato de trabajo no haya consentimiento que valga, pues eso no es así. Con ello se desea dar al consentimiento la importancia que merece y valorarlo ante el tratamiento y uso de los datos por parte del empresario en el seno de la relación laboral. Es aquí, en la LOPD donde se encuentra la respuesta a los límites del uso del empresario de esos datos personales, y no en el Estatuto de los Trabajadores.

IV. Estudio de la norma estatutaria y su necesaria reflexión a la luz del Reglamento y de la Ley Orgánica de Protección de Datos

47. La potestad de dirección y control de la actividad laboral regulada en el artículo 20.3 del Estatuto de los Trabajadores permite al empresario adoptar las medidas que estime oportunas para que el trabajador cumpla con sus obligaciones y deberes laborales, una potestad que ha intensificado expo-

³³ Sobre esta concepción C. CONDE ORTIZ, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005.

³⁴ En este sentido, se pronuncian las SSTC 94/1998, de 4 de mayo; 292/2000, de 30 de noviembre. Así lo señala la propia Exposición de Motivos de la LOPD.

³⁵ Cfr. J. L. GOÑI SEIN “Nuevas tecnologías digitales...”, op. cit. p. 4.

nencialmente el uso de la tecnología. A pesar de ello, recoge como único límite la adopción y aplicación de medidas de control que guarden la debida dignidad a los trabajadores, sin otra concreción mas allá de que se tenga en cuenta la capacidad real de los trabajadores con discapacidad. La previsión es equivalente a la redacción dada en los años noventa, en los que no se contaba con un entorno digital y tecnológico tan invasivo (y económico) de la intimidad del trabajador.

48. No es ajeno al lector que la norma estatutaria ya es tachada de adolecer de claros síntomas de insuficiencia al no ofrecer concreción al conflicto jurídico que suscita la tecnología, pues no marca el equilibrio entre el derecho empresarial a controlar la actividad laboral de sus empleados con la posible afectación a los intereses jurídicos de los trabajadores, como el derecho a la intimidad (artículo 4.2.e) del Estatuto de los Trabajadores), el derecho a la intimidad personal y familiar (artículo 18.1 de la Constitución Española), y el derecho a la privacidad y al secreto de las comunicaciones. Así, a pesar de la adopción de la LOPD, lo cierto es que, “el conflicto jurídico suscitado por las nuevas tecnologías digitales se mantiene huérfano de solución en nuestro ordenamiento jurídico laboral. No existe una normativa específica que contemple de alguna manera los problemas derivados de la utilización de los medios técnicos como mecanismos de control en el lugar de trabajo. El legislador ha omitido sistemáticamente en todas las reformas laborales, el tratamiento de los nuevos derechos vinculados al desarrollo de las TIC, pese a los delicados problemas aplicativos suscitados”³⁶.

49. A pesar de esta inercia, el único paso dado por el legislador español en la regulación de los derechos digitales ha sido la inclusión en el Estatuto de los Trabajadores de un nuevo artículo 20 (bis) para concretar que los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales³⁷. Desde luego, la incorporación de este precepto en la norma estatutaria es un pequeño y tímido paso en la necesaria tarea de limitar de algún modo la invasión a la intimidad de los trabajadores producto de la era digital y de las tecnologías. Ahora bien, la escasa concreción del artículo 20 bis cabría completarla con las disposiciones de la LOPD.

50. Por un lado, es plausible el paso dado por el legislador al formular una regulación legal que trata de dotar de una mayor seguridad jurídica. Así, los artículos 87 a 90 de la LOPD disponen el alcance y la extensión de los derechos reconocidos en el artículo 20 bis del Estatuto de los Trabajadores: a la intimidad y uso de dispositivos digitales en el ámbito laboral; a la desconexión digital en el ámbito laboral; a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo; y a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral³⁸.

51. Por otro lado, la LOPD otorga un rol complementario a la autonomía colectiva al exponer que “Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral”³⁹.

³⁶ Vid J. L. GOÑI SEIN, “Nuevas tecnologías digitales...”, op. cit. p. 8.

³⁷ Este precepto fue introducido por la Disposición Final decimotercera de la LOPD.

³⁸ Vid. S. RODRÍGUEZ ESCANCIANO, “Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales”, *Diario La Ley*, núm. 9328, 2019.; R. TASCÓN LÓPEZ, “Big Data y Relaciones laborales: reflexiones sobre la protección de datos generados en el lugar de trabajo a la luz de los cambios de paradigma sociales y legales” (Coord.: S. RODRÍGUEZ ESCANCIANO), En *Proyección transversal de la sostenibilidad en Castilla y León: varias propuestas*, pp. 339-390, 2019; P. BURRIEL RODRÍGUEZ-DIOSDADO, “El desnudo integral genético en el mundo laboral: Revolución industrial 4.0” *Revista Internacional y Comparada de Relaciones Laborales y Derecho del empleo*, núm. 1, 2018, pp. 64-93.

³⁹ Artículo 91 de la LOPD. Será clave este precepto para enlazarlo con el epígrafe correspondiente al rol desempeñado por los representantes de los trabajadores.

52. Como bien se ha expresado por la doctrina, esta Era Digital y tecnológica han ido forjando una realidad “absolutamente impensable para una legislación laboral como la española que, en sus aspectos esenciales, y aún reformada en múltiples aspectos, procede en esencial del siglo pasado”⁴⁰. Es por tanto que las comunicaciones en las relaciones laborales, la potestad de control empresarial y el mismo derecho a la intimidad de los trabajadores ha quedado muy alejado de la visión del legislador español del siglo pasado. Así, éste no ha sido capaz de adaptar la normativa laboral a la realidad que reina en una sociedad laboral española globalizada y tecnológica.

1. El rol de los representantes de los trabajadores en la Era Digital

53. El RGPD, aunque aplicable a las relaciones de trabajo, ni encaja ni está diseñado para atender la problemática que acaece en las relaciones laborales. Así, es tachado de un carácter individualista en el que los derechos son otorgados a la persona del trabajador sin atender ni relacionarlo con los derechos colectivos y sin considerar las funciones de vigilancia y control de los representantes de los trabajadores. En cualquier caso, el RGPD no es una norma específica y concreta de la protección de datos en el orden laboral dificultando el encaje de esta norma a las relaciones laborales con total plenitud⁴¹.

54. La misma crítica se puede elevar para la LOPD que presenta “un casi completo vacío en la regulación del Derecho colectivo digital en las relaciones laborales (...). La transmisión de la información sindical, los derechos de consulta y participación, el papel de la negociación colectiva en cada uno de los derechos digitales, la definición de los sindicatos como cesionarios de los datos personales; la necesaria ponderación entre protección de datos y libertad sindical, Las acciones colectivas en defensa de los derechos a la protección de datos en la empresa (...) permanece aún en el tintero del olvido - nada involuntario -de nuestro legislador (...)”⁴².

55. En efecto, el RGPD es ajeno a la realidad social y económica que impera en la sociedad capitalista que asigna unos roles diferenciados a las partes del contrato de trabajo, con poderes de negociación distanciados entre trabajador y empresario. En base a esta realidad y en aras del carácter tuitivo del Derecho laboral es necesario que existan representantes de los trabajadores que defiendan los intereses de los trabajadores en la Era Digital. En este momento, téngase presente que la defensa de estos intereses es necesaria ante la gestión automatizada de sus datos personales y ante las decisiones automatizadas que afecten a aspectos tan importantes como una sanción o un despido. Y ello porque se hace difícil y complejo que un trabajador de forma individual se pueda oponer a que sus datos personales sean automatizados o a que se tomen decisiones automatizadas que les perjudiquen.

56. Aun a pesar de la ausencia de auténticas previsiones sobre los derechos colectivos de los trabajadores, lo cierto es que el artículo 80 del RGPD dispone que el interesado tiene derecho a ser representado por una entidad, organización o asociación que actúe en el ámbito de la protección de sus derechos y libertades en la materia de protección de sus datos personales. La actuación de esta institución, que podría ser perfectamente la representación de los trabajadores, se enmarca en presentar en el nombre del interesado una reclamación ante la autoridad de control si considera que el tratamiento de los datos personales infringe la norma europea. Es evidente que el interesado (o su representante) puede hacer valer los derechos vulnerados (derechos de acceso, rectificación, oposición, etc.) ante la Agencia

⁴⁰ Cfr. F. J. CALVO GALLEGU, “TIC y poder empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y Redes Sociales”, *Aranzadi Social: Revista Doctrinal*, Vol. 4, núm. 9 (ene), 2012, p. 127.

⁴¹ Es interesante lo señalado por M. B. CARDONA RUBERT, “Tratamiento automatizado de datos personales del trabajador”, *Revista de Trabajo y Seguridad Social*, núm. 16 1994, pp. 83-118; L.A. FERNÁNDEZ VILLAZÓN, “Tratamiento automatizado de datos personales en los procesos de selección de trabajadores”, *Relaciones Laborales*, núm. 1, 1994, pp. 510-538; A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos...”, op. cit. p. 81.

⁴² Cfr. C.H. PRECIADO DOMÉNECH, “La Era digital y la vieja economía nueva”, *Revista de la Comisión de lo Social de Jueces y Jueces para la Democracia*, núm. 197, 2019, p. 71.

Estatal de Protección de Datos, sin perjuicio de la posibilidad de acudir a la vía judicial. En esta línea, la Agencia permite atender reclamaciones por la presunta vulneración del tratamiento de los datos personales. Para ello, el afectado o su representante tendrá que imponer una queja especificando los motivos en el modelo de solicitud habilitado al efecto en el que se aporten los indicios necesarios que les permitan investigar. Ahora bien, de forma previa, debe dirigirse a la entidad responsable del tratamiento de los datos personales⁴³.

57. No obstante, la cuestión sería discernir si los representantes de los trabajadores necesitan la autorización expresa del trabajador para poder conocer del asunto (y no solo conocer, sino para poder gestionar el derecho a la protección de los datos de los trabajadores en una supuesta situación de tratamiento indebido o ilícito). En este aspecto, se puede plantear si podría ejercer este derecho por parte del sindicato en relación a sus afiliados, sin necesidad de una declaración expresa o acción afirmativa de éstos⁴⁴.

En línea de los procesos judiciales de solución de este tipo de conflictos, y en cuanto a la representación y defensa procesales, los sindicatos pueden actuar en un proceso, en nombre e interés de los trabajadores para la defensa de los derechos individuales de éstos. En este término se aclara que “la autorización se presumirá concedida salvo declaración en contrario del afiliado”⁴⁵. En cualquier caso, se exige que el sindicato comunique al afiliado su voluntad de iniciar el proceso. De hecho, si el afiliado expresa en la oficina judicial que no ha recibido esa comunicación del sindicato, o aún recibéndola se ha negado a iniciar el proceso, “el juez o tribunal, previa audiencia del sindicato, acordará el archivo de las actuaciones sin más trámite”⁴⁶.

58. Con respecto a este aspecto, se ha interpretado que en el seno de la función de vigilancia y control que tiene reconocida la representación unitaria se incluye la reclamación de los derechos individuales en el seno de la empresa y ante las autoridades y tribunales⁴⁷. En esta línea argumental, se ha formulado que “impedir la capacidad para formular acciones legales sería vaciar de contenido sus funciones legalmente reconocidas”⁴⁸. De la manera relatada, la representación unitaria necesitaría de la habilitación expresa en forma de consentimiento por parte del trabajador afectado. No obstante, es muy interesante subrayar que no solo les cabe actuar en juicio, pues tienen reconocidas otras competencias más incisivas y más directas en la gestión de la información por el empresario, como es el derecho de información.

59. En este punto, nos podríamos plantear si es necesario que el trabajador preste su consentimiento a los representantes de los trabajadores para que éstos conozcan del algoritmo, y consecuentemente, los datos personales del trabajador. Ello se tendrá que poner en coalición con el derecho de información de los representantes de los trabajadores del artículo 64 del Estatuto de los Trabajadores. Este precepto recoge el deber empresarial de suministrar información de carácter laboral y/ o profesional a aquellos. En este aspecto, la doctrina ya se ha encargado de precisar que tal entrega no requiere consentimiento expreso y específico del trabajador contratante. Esta matización descansa, como bien se ha encargado de subrayar esa doctrina, en razones de legalidad basadas en la “constatación jurídico-práctica de que el trabajador asume de ordinario la condición de sujeto más débil”. Ante esta realidad, “la exigencia de consentimiento previo del trabajador supondría, en realidad, un elemento decisivo

⁴³ Información disponible en <https://www.aepd.es/es> (Último acceso: 1 de marzo de 2020). Vid. E. GIL, *Big Data, privacidad y protección de datos*, Agencia Estatal Boletín Oficial del Estado, Madrid, 2016

⁴⁴ El propio artículo 80 del Reglamento no hace mención alguna a la exigencia de una habilitación expresa por parte del trabajador a los representantes en este extremo.

⁴⁵ Cfr. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos ...”, op.cit., p. 78.

⁴⁶ Artículo 20 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (BOE núm. 245 de 11 de octubre de 2011). Vid. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos ...”, op.cit. p. 78.

⁴⁷ Vid. R. I. PALOMO VÉLEZ, “Algunas consideraciones sobre las competencias de los representantes legales de los trabajadores”, En *Comentarios al Estatuto de los Trabajadores: libro homenaje a Tomás Sala Franco*, Tirant lo Blanch, Valencia 2016, pp. 1211-1224.

⁴⁸ El artículo 20 de la Ley Reguladora de la Jurisdicción Social nombra el derecho de representación procesal de los sindicatos, que no de la representación unitaria. Vid. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos ...”, op.cit. p. 82.

para la ineffectividad del deber, habida cuenta la incontestable posición de supremacía contractual del empresario”⁴⁹. Así pues, es preciso que los riesgos que comporta esta Era, la afectación a los derechos fundamentales de la persona y del trabajador, cuenten con un marco jurídico eficiente como para adaptarse a la rapidez y a la intensidad inherente a la Era Digital.

60. Ante la tesitura planteada, nos podríamos cuestionar si las reformas en relación a la intervención de los representantes para la protección de los derechos de los trabajadores deben venir de la norma estatutaria, o si, por el contrario, esta debe ceder su espacio a la autonomía colectiva por contar esta última con una capacidad de reacción más rápida a la hora de adaptarse a las necesidades de esta nueva Era en el Derecho del Trabajo. Es decir, si la sociedad digital y su afectación a los derechos laborales (en este caso, el derecho a la protección de datos y su influencia en los derechos de información y consulta) presenta tanto dinamismo como los riesgos a proteger, de modo que deba ser la negociación colectiva la encargada de dotar a éstos de una protección adecuada.

2. La autonomía colectiva en la Era Digital

61. Un riesgo importante de la Era digital y en la dictadura de los datos es el debilitamiento del poder de negociación y de la función de vigilancia y control de los representantes de los trabajadores habida cuenta que el propio RGPD no considera los derechos colectivos. A pesar de esta limitación, si se puede celebrar que el RGPD da pequeños pasos en relación a la autonomía colectiva. A continuación, se exponen los preceptos a tal fin dirigidos.

62. Un aspecto positivo es que el RGPD invoca a los Estados a regular disposiciones legislativas y a invitar a los convenios colectivos a establecer normas más específicas para garantizar la protección de los derechos y las libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral.

63. En efecto, el Considerando núm. 155 del Reglamento da un pequeño paso respecto a la Directiva 95/46/CE y expone que *El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.*

64. Otro aspecto a destacar es que el RGPD excluye como “categoría especial de datos personales” cuando el tratamiento sea necesario para el cumplimiento de las obligaciones y del ejercicio de los 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 interesado⁵⁰.

⁴⁹ Cfr. S. RODRÍGUEZ ESCANCIANO, “Los riesgos del denominado “data outsourcing” en el proceso de colocación: límites a la cesión de información entre los posibles sujetos intervinientes”, *Revista Internacional y Comparada de Relaciones Laborales y Derecho del empleo*, Vol. 7, núm. 2, abril-junio, 2019. La autora se refiere a la copia básica del contrato de trabajo. En relación a la supremacía del empresario J. L. MONEREO PÉREZ, *Los derechos de información de los representantes de los trabajadores*, Civitas, Madrid, 1992.

⁵⁰ Vid. artículo 9.2 b) del RGPD.

Ello viene a significar que cuando concurra esta circunstancia no se aplicará, en principio, la prohibición de tratamiento de los datos personales enunciada en el artículo 9.1 del RGPD.

65. Luego, como última referencia que el RGPD alude al Convenio, es cuando de forma particular recoge que los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y de las libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral. Esta previsión legislativa y convencional la dispone con amplitud, y de forma particular, el RGPD nombra aspectos esenciales de la relación de trabajo como son los efectos en la contratación de personal, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, la gestión, la planificación y la organización del trabajo, la igualdad y la diversidad en el lugar de trabajo, la salud y la seguridad en el trabajo, la protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y de las prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

Es más, las normas de los Estados tendrían que incluir medidas adecuadas y específicas para preservar la dignidad de los trabajadores y sus intereses legítimos, así como sus derechos fundamentales. En cualquier caso, el único aspecto que detalla el RGPD es que los Estados deben prestar especial atención a la transparencia tanto del tratamiento, como de los datos personales, así como a los sistemas de supervisión en el lugar de trabajo⁵¹.

Este anuncio se podría relacionar con el carácter complementario de los convenios colectivos. De esta manera, cabe recordar que la LOPD otorgaba un rol complementario a la autonomía colectiva al indicar que podrían establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral⁵².

66. Este llamamiento es adecuado considerando el carácter genérico de la norma sobre protección de datos personales que hace cuestionar seriamente la suficiencia de la misma en el orden de las relaciones laborales. Para superar esta insuficiencia normativa, es clave la actuación de los interlocutores sociales a fin de que adopten acuerdos y convenios para tutelar los derechos de los trabajadores en la Era Digital. A pesar de este llamamiento, del gran margen de maniobra que le concede el RGPD y de esta necesidad, lo cierto es que es escasa la reacción al respecto. Se podría empezar a presumir la inacción de los interlocutores sociales en este aspecto, aún a pesar de la premura en esta conclusión teniendo en cuenta el tiempo transcurrido desde la entrada en vigor del RGPD y de la LOPD, 2016 y 2018.

67. En cualquier caso, a fecha de hoy, y haciendo un rastreo de los convenios más actuales, son pocos los que recogen cláusulas relativas a la protección de los datos personales, y en consecuencia son escasos los ejemplos de iniciativas convencionales en la materia que aquí podrían citarse.

68. En algún caso⁵³, la voluntad de los interlocutores sociales se limita a disponer de un marco protector para la empresa, al señalar que todos los trabajadores están obligados a respetar la Ley de Protección de Datos. En el mismo sentido, incorpora el deber de confidencialidad y de secreto de la información para todos los trabajadores durante la prestación de servicios (incluso tras la extinción de su relación laboral). Estos deberes alcanzan a aquella información que sea recibida por su prestación de servicios, así como cualquier otra información generada por su propia actividad. También se prevé la limitación a lo estrictamente laboral en la utilización de los recursos informáticos (correo electrónico, navegación por

⁵¹ Vid. artículo 88 del RGPD.

⁵² Artículo 91 de la LOPD. Comentábamos que este precepto sería clave este precepto para enlazarlo con el epígrafe correspondiente al rol desempeñado por los representantes de los trabajadores. Sobre la regulación de los derechos “tecnológicos” en la negociación colectiva A. BAYLOS GRAU, “El papel de la negociación colectiva en la ley de protección de datos personales y garantía de derechos digitales en España”, *Labour & Law Issues*, Vol. 5, núm. 1, 2019.; J. M. SERRANO GARCÍA, *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, Editorial Bomarzo, Albacete, 2019.

⁵³ Artículo 32 del Convenio Colectivo 2020-2023 de la empresa Drylock Technologies SL (Boletín Oficial De La Provincia De Segovia, núm. 25 de 26 de febrero de 2020).

internet). Para asegurar la correcta utilización de las herramientas y de los dispositivos informáticos, se advierte que la empresa podrá vigilar, controlar y monitorizarlos. Como se aprecia, el Convenio recurre a la Ley de Protección de Datos para atender los intereses de la empresa, pero no se pronuncia con respecto a posibles vulneraciones que se puedan dar por parte de la misma a sus empleados en relación a la protección de datos, más allá de señalar el carácter confidencial de las credenciales para el acceso a los sistemas y la prohibición de acceso al sistema de quién no esté debidamente autorizado.

69. En otro caso⁵⁴, el convenio advierte que los trabajadores deben quedar informados de la incorporación de sus datos a los ficheros existentes en la empresa para el mantenimiento de su relación contractual y para las finalidades del propio cumplimiento del convenio. Desde luego, nos parece del todo acertado que este Convenio señale concretamente que los trabajadores deben autorizar que sus datos personales sean facilitados a los representantes de los trabajadores para los fines previstos en la legislación vigente (entiéndase, para la función de vigilancia y control). En la misma línea, este convenio establece que los ficheros creados estarán bajo la supervisión y control de la empresa, ante los cuales los trabajadores podrán ejercer los derechos de acceso, rectificación, cancelación y oposición en la forma prevista en la legislación vigente. Como se puede apreciar, y hasta aquí este convenio trata de tutelar los intereses de los trabajadores afectados. Además, este convenio hace referencia a los datos sensibles a los que tienen acceso los trabajadores y dispone que están especialmente obligados al secreto profesional respecto a los datos de carácter personal, tal y como se definen en la LOPD y en el RGPD. Del mismo modo, los trabajadores han de cumplir y respetar las medidas generales de seguridad que la empresa establezca respecto de los ficheros que contengan datos personales. Por último, este convenio establece ciertas normas con respecto al uso de las nuevas tecnologías en el trabajo para advertir que la utilización del correo electrónico y de la navegación por internet sólo está permitida por motivos estrictamente laborales y el uso y control de los ordenadores y de los programas informáticos instalados y facilitados por las empresas quedará limitado exclusivamente por razones de trabajo, siendo el trabajador el único responsable de la custodia de las claves de acceso utilizadas para su trabajo, las cuales son personales e intransferibles.

70. Una previsión convencional⁵⁵, relaciona la tecnología con la organización del trabajo como factor del poder de dirección empresarial y viene a señalar que “La organización del trabajo en cada una de las empresas es facultad de la dirección de la misma, de acuerdo con lo previsto legal y convencionalmente. El sistema de racionalización, mecanización y dirección del trabajo que se adopte, nunca podrá perjudicar la formación profesional que el personal tiene derecho a completar y a perfeccionar por la práctica debiendo ser consultados los representantes de los trabajadores en todas aquellas decisiones relativas a tecnología y organización del trabajo”.

71. Otra previsión convencional en relación a los datos personales del empleado precisos para la prestación del servicio (domicilio, teléfono, estado civil, número de personas a su cargo, etc.) es asegurar en términos absolutos su confidencialidad y el adecuado uso de los mismos con el debido respeto a la norma legal e interna de la empresa. Así, los datos médicos facilitados por el empleado, por cualquier circunstancia, al servicio médico de la empresa solo podrán ser utilizados para los fines para los que se facilitaron⁵⁶.

72. Siguiendo con este análisis, se dan también previsiones convencionales que se limitan a recoger, sin más precisión, la protección de datos personales de las personas trabajadoras y el derecho a su desconexión digital a fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar⁵⁷.

⁵⁴ Artículo 46 del VI Convenio autonómico de Pompas Fúnebres de Galicia. Diario Oficial de Galicia 15 abril 2019, núm. 73.

⁵⁵ Capítulo II del II Convenio colectivo estatal del comercio minorista de droguerías, herboristerías y perfumerías (BOE, núm. 192 de 12 de agosto de 2017).

⁵⁶ Artículo 23 VII Convenio colectivo de Diario ABC, SL. (BOE núm. 50 de 27 de febrero de 2020).

⁵⁷ Artículo 43 del Convenio colectivo para la empresa Fundación Estadio Vital Fundazio (Boletín Oficial del Territorio Histórico de Álava, 2 de marzo de 2020).

73. También se puede apuntar otras previsiones recogidas en convenio⁵⁸, que se limitan a exponer que la implantación de tecnología de información para el control de la prestación laboral, tales como controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador (monitorización remota, indexación de la navegación por internet, o la revisión o monitorización del correo electrónico y/o del uso de ordenadores) o los controles sobre la ubicación física del trabajador mediante geolocalización, se realizará respetando en todo momento las previsiones normativas, deberán ser proporcionales para verificar el cumplimiento por parte del trabajador de sus obligaciones laborales, respetando su dignidad y su derecho a la protección de datos y a su vida privada. Sin embargo, este convenio señala que, teniendo en cuenta, que la legitimación para el tratamiento deriva de la existencia de la relación laboral, no se requiere del consentimiento del trabajador. Al respecto al deber de información, expone que se debe informar al trabajador y, que cuando, este tipo de medidas tengan el carácter de colectivas o plurales deberá informarse previamente a su implantación a los representantes de los trabajadores, indicando la finalidad que se persigue. Un ejemplo de esta información es en relación a los sistemas de videovigilancia para el control periódico y regular de la prestación laboral (artículo 8). Si que recoge deberes de información (y de consulta) en relación a la introducción de nuevas tecnologías que supongan una modificación sustancial de las condiciones de trabajo o la necesidad de un periodo de formación (artículo 10). Si puede resultar interesante apuntar que recoge un deber de consulta a los representantes de los trabajadores sobre aquellas decisiones relativas a la tecnología organización del trabajo y utilización de materias primas que tengan repercusión sobre la salud física y/o mental del trabajador (artículo 36). A pesar del carácter innovador que suele presentar este convenio, y del alto valor que les da a las nuevas tecnologías, nada señala en relación al deber de informar sobre la toma y el tratamiento de los datos de los trabajadores vinculados a las nuevas tecnologías.

Otras previsiones convencionales se centran en la actuación de los representantes de los trabajadores en esta materia⁵⁹. Así se ha previsto el uso por el Comité Intercentros de una página en la Intranet de la Empresa para la publicación de información de carácter sindical. Además, se le facilita a Secciones Sindicales y a sus Coordinadores y Secretarios Generales, todos los medios necesarios (medios informáticos, telefónicos, etc.) para poder desarrollar su representación sindical dentro de la Empresa. De esta manera, se potencia el derecho de información de la representación de los trabajadores en su vertiente activa con la utilización de las nuevas tecnologías de la información como medio de comunicación con sus representados.

74. Un último convenio al que acudimos⁶⁰, se pronuncia sobre aspectos algo más relevantes, al establecer, “Sin perjuicio de los derechos de información de los Órganos de representación unitaria de las personas trabajadoras de cada una de las Empresas, en las reuniones que se celebren entre la Comisión Directiva de las Empresas y los Sindicatos más representativos, y que tendrán una periodicidad trimestral como mínimo, la Dirección informará sobre las líneas básicas y estrategias de la evolución del conjunto de las tres Empresas: introducción de nuevas tecnologías, evolución de las redes y servicios, aspectos organizativos, comerciales, legales, y contratas, recursos humanos” (artículo 8). Por otro lado, y en relación al nivel de confidencialidad y secreto sobre la información de la empresa, se estipula que “Todas las personas trabajadoras se obligan, durante la prestación de servicios a la Empresa e incluso tras la extinción de su relación laboral, a mantener la más estricta confidencialidad y secreto sobre la información no pública como consecuencia de su relación de laboral en favor de la misma, así como sobre cualquier otra información que utilice por su propia actividad, a través de las distintas herramientas informáticas puestas a su disposición. Al cesar en la Empresa, los archivos que se reciban en las herramientas tecnológicas de la persona trabajadora que cesa, o que estén almacenados en la misma, son

⁵⁸ Convenio Colectivo general de la industria química (BOE núm. 191 de 8 de agosto de 2018).

⁵⁹ Artículo 49 del Convenio colectivo de Siemens Healthcare, SLU. (BOE núm. 51, de 28 de febrero de 2020). Sobre la utilización de los medios tecnológicos por parte de los sindicatos F.A. Valle Muñoz, “La incidencia de las nuevas tecnologías en la transmisión sindical de información en la empresa”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 52, 2019, pp. 136-182.

⁶⁰ II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU (BOE núm. 273 de 13 de noviembre de 2019).

de uso profesional, por lo que la Empresa tendrá libertad para su revisión o eliminación” (artículo 168). En relación al nivel de información de las tecnologías, el convenio vincula el deber de información a la prevención de riesgos laborales y a la salud laboral al señalar que “Los miembros de los Comités de Seguridad y Salud conocerán antes de su puesta en práctica, en lo referente a prevención de riesgos, los nuevos métodos de trabajo y especialmente aquellos que impliquen la utilización de nuevas tecnologías. Estos métodos de trabajo deberán ser informados en el seno del Comité de Seguridad y Salud.” (Disposición Adicional Cuarta).

75. Desde luego, la regulación contenida en los convenios se limita a expresiones relacionadas con limitaciones o concreciones en el uso de las nuevas tecnologías por parte de los trabajadores o de la intranet por parte de la representación de los trabajadores. Es más, suelen acoger un régimen disciplinario bastante intenso en relación a incumplimientos laborales y a las nuevas tecnologías en relación a posibilidades de instalación de videocámaras o de cualquier otro dispositivo de control de la prestación laboral, tanto en el cuerpo del empleado, como en los recursos informáticos que emplea, sean propiedad de la empresa o no, siempre que sean usados para fines distintos de lo estrictamente laboral. Conjuntamente, los convenios colectivos se pronuncian al respecto de las nuevas tecnologías, pero en relación a la necesidad de formación, a la necesidad de incorporar nuevas pautas preventivas en aras a garantizar la seguridad del trabajador, e incluso, a la posibilidad y el procedimiento para que puedan ser modificaciones sustanciales de las condiciones de trabajo o que supongan la extinción del contrato por ineptitud del trabajador. En este punto, no hemos encontrado instrumentos convencionales que recojan obligaciones informativas en relación al uso de los algoritmos, ni siquiera que se pronuncien sobre las consecuencias jurídicas de un uso desviado e ilícito de los algoritmos en relación a los candidatos-trabajadores que pudieran quedar afectados por decisiones automatizadas o semi-automatizadas.

76. Como se puede apreciar, consideramos que es esencial realizar un llamamiento para que los representantes de los trabajadores sean conscientes de la necesidad de articular medidas tuitivas que preserven los derechos fundamentales que pueden verse afectados en la relación de trabajo, como son el derecho a la intimidad, a la dignidad y el derecho de protección de datos personales.

77. Por lo demás, los interlocutores sociales deben promocionar el interés legítimo de los trabajadores en cuanto a controlar sus datos personales que circulan en los sistemas de comunicación e información. De hecho, “solo así puede ejercer un seguimiento sobre el uso secundario de esos datos y evitar la afectación negativa durante la relación laboral o su postergación para el empleo”⁶¹.

78. En este escenario, los convenios colectivos no predicen nada con respecto a la obligación empresarial de informar, consultar, ni negociar con los representantes de los trabajadores sobre su actuación ante la protección de datos personales y su posible vulneración por las daciones automatizadas. Como no existe un marco normativo laboral que proteja los derechos de los trabajadores ante posibles injerencias en sus datos personales no justificadas y que sean constitutivas de decisiones discriminatorias se propone como *lege ferenda* la siguiente propuesta.

3. Los derechos de información y consulta en la Era Digital: el traslado de la funcionalidad del derecho de información como refuerzo del deber de secreto y de sigilo profesional

79. Existe un conflicto permanente entre los recelos empresariales al derecho a la protección de datos con los derechos de información y consulta, que ha sido una fuente continua de resoluciones judiciales. Estas tienen su origen en el “excesivo celo de las empresas, que ven en la protección de datos

⁶¹ Cfr. S. RODRÍGUEZ ESCANCIANO, “Participación de los representantes de los trabajadores en el tratamiento de los datos personales: Derechos de información y consulta”, *Revista de la Comisión de lo Social de Juezas y Jueces para la democracia*, núm. 197, 2019, p. 7.

un fiel aliado para ocultar a los representantes unitarios o sindicales datos relevantes para el ejercicio de su función; otras veces porque dichos representantes se exceden en sus funciones y quieren conocer datos respecto de los que existen derechos fundamentales de los trabajadores que los ponen a salvo de cualquier transmisión sin su consentimiento”⁶².

80. En esta sede de análisis, se concluye que la norma estatutaria precisa de un completo proceso de adaptación a la Era Digital y tecnológica que afecta al mercado de trabajo. En concreto, y considerando la velocidad vertiginosa con la que acaecen los cambios tecnológicos y la incapacidad del legislador para atender todos los aspectos relacionados con posibles injerencias empresariales, lo que sí debe hacer la norma estatutaria es recoger normas vinculantes para que las empresas se vean obligadas a buscar la colaboración y acuerdo de los representantes de los trabajadores en las cuestiones que hemos señalado. Es por esto que los interlocutores deben sentarse a negociar para acordar cláusulas obligacionales convencionales en este extremo.

81. Ello se traduce en que los representantes de los trabajadores tengan derecho a conocer la lógica del algoritmo, la gestión y tratamiento de los datos considerados en la formulación concreta. Que sea conocida la lógica informática del algoritmo es necesaria no solo de cara a evitar situaciones y sesgos discriminatorios, incluso de cara a superar la dificultad de hacer entender al trabajador esta compleja fórmula⁶³. Este derecho se tendría que incorporar al artículo 64.5 del Estatuto de los Trabajadores. Del modo dibujado, la capacidad de actuación de la empresa (en orden a la protección de datos personales) se encontraría limitada por la intervención, vigilancia y control de los representantes⁶⁴.

82. En definitiva, se trata de un control *intra* proceso desde la propia formulación del algoritmo, desde la recapitulación y el tratamiento de los datos personales para que sean utilizados con un fin legítimo y adecuado. Este control permitiría conocer la legalidad y legitimidad de las decisiones que toman las empresas con base en los datos de los trabajadores tratados por un algoritmo. De esta forma, los representantes de los trabajadores, y por este medio de información, los trabajadores, podrían conocer que la empresa automatiza sus datos personales (el alcance y el grado de la automatización, podrían controlar el cumplimiento de la norma al gozar de la explicación lógica que preside la toma de cualquier decisión empresarial basada en algoritmos. Ello ha sido calificado por la doctrina como gobernanza colectiva de los derechos de la protección de datos por parte de los representantes de los trabajadores. Esta gobernanza alcanza a todos los aspectos de la relación laboral desde sus inicios (proceso de selección, proceso de contratación, evaluación del desempeño, ascensos y promoción o extinción del contrato). Se trata, por tanto, de ampliar los derechos de información, consulta y de negociación de los interlocutores sociales. En este sentido, el propio RGPD en su artículo 88 abre la vía para que se establezcan normas más específicas para garantizar la protección de datos en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral a través de convenios colectivos. Desde luego, es la mejor opción para garantizarse con transparencia y objetividad que no existen discriminaciones o sesgos en las

⁶² Cfr. C. H. PRECIADO DOMÈNECH, “La aplicación judicial de los derechos de información, consulta y control sindical”, *Ian Harremanak*, II, 2016, p. 98.

⁶³ Este apunte se puede relacionar con “el denuedo empresarial en cumplir de buena fe con los deberes informativos que el asigna el RGPD”. Cfr. A. VILLALBA SÁNCHEZ, “El principio de transparencia en la ejecución automatizada del contrato de trabajo: una aproximación jurídica a la tecnología “blockchain” y a la inteligencia artificial”, *Nueva revista española de derecho del trabajo*, núm. 224, 2019, pp. 183-226. A su vez, hay que subrayar la dificultad técnica de hacer entender la decisión que ha tomado el programa informático junto a la falta de entendimiento de estos sistemas. Ante estos supuestos, la doctrina recomienda que quienes sean las encargadas de tratar estos datos hayan sido lo suficientemente formadas para poder explicar o tratar de explicar estas decisiones. Vid. A. PALMA ORTIGOSA, “Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos”, *Revista General de Derecho Administrativo*, núm. 50, 2019

⁶⁴ Los derechos de información y consulta vienen a establecer unos límites a los poderes empresariales, y un instrumento para ampliar las funciones negociales. Al respecto, E. GARRIDO PÉREZ, *La información en la empresa. Análisis jurídico de los poderes de información de los representantes de los trabajadores*. CES, Madrid 1995, especialmente, pp. 261-286.; S. RODRÍGUEZ ESCANCIANO, “La participación en la gestión empresarial a través de la contratación colectiva”, comunicación presentada en el *XVII Congreso nacional de AEDTT*.

decisiones tomadas en base al *Big Data*⁶⁵. Esta gobernanza colectiva evitaría que el empresario de forma individual y unilateral arbitre cualquier medida para proteger los derechos de los trabajadores. Así, tendría que acordar con los representantes de los trabajadores la fórmula, los métodos y las salvaguardas para proteger a los mismos frente a la gestión, al tratamiento y al procesamiento automatizado de los datos de los candidatos/trabajadores.

83. En este sentido, se entiende que, dado que el RGPD impone una obligación de resultado, garantizar el derecho de protección de los datos personales, y considerando que esta obligación queda en manos del responsable de los datos en la empresa que goza de libertad para establecer los métodos y las salvaguardas para cumplirlo. Esta formulación y potestad unilateral tiene sentido en el ámbito de los consumidores porque existe poca representatividad de las asociaciones de los consumidores, pero no está justificada en el escenario de las relaciones laborales donde se cuenta con unas instituciones plenamente aceptadas y con legitimidad suficiente para actuar en este terreno⁶⁶.

84. En orden a incorporar esta “nueva” obligación empresarial de informar y consultar a los representantes de los trabajadores sobre las medidas de salvaguardas y medidas en el orden laboral de la protección de datos, y como parte integrante de los derechos de información y consulta recogidos en el artículo 64 del Estatuto de los Trabajadores⁶⁷. Se trata de diseñar mecanismos que garanticen la información (y la participación) de los representantes de los trabajadores para evitar la inclusión de sesgos discriminatorios y modelos de gobernanza deficientes. Desde luego, podría manifestarse este derecho de información y consulta ante las decisiones de la empresa que pudieran provocar cambios relevantes en cuanto a la organización del trabajo en la empresa; e incluso dentro del derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre cuestiones como la implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo.

85. En este punto, téngase presente que los dispositivos tecnológicos y digitales son utilizados como un instrumento no solo de la gestión del personal, sino que se emplean en el círculo rector del poder de dirección y disciplinario de la empresa. De hecho, son instrumentos verificadores del cumplimiento laboral, y también “magníficos medios de prueba, que permiten acreditar el incumplimiento de sus obligaciones laborales por el trabajador en el proceso laboral. Los instrumentos tecnológicos pueden ser preordenados con un fin disciplinario; en la casuística de los tribunales se encuentran a menudo casos de utilización de las cámaras de video-vigilancia o de dispositivos de geolocalización para obtener la prueba de alguna conducta irregular del trabajador en el desempeño de su actividad laboral sea dentro o fuera de la empresa”⁶⁸. Si la tecnología se dispone como medio de prueba del empresario, nada impide que también pueda ser empleada por la representación de los trabajadores en el ejercicio diario de su función de control y vigilancia de cara a evitar la indefensión del trabajador y a hacer efectivo el derecho a la tutela judicial efectiva.

⁶⁵ Esta posición estaría en línea con los requisitos esenciales enunciados en las Directrices éticas para una inteligencia artificial fiable elaboradas por el grupo de expertos de alto nivel sobre inteligencia artificial, como son la transparencia, la privacidad de datos, la intervención y la supervisión humanas, la no discriminación. Vid. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Regiones, Generar confianza en la inteligencia artificial centrada en el ser humano, COM (2019) 168 final, Bruselas, 8.4.2019. De hecho, este documento anuncia que “deben garantizarse la privacidad y la protección de datos en todas las fases del ciclo vital del sistema de IA. Los registros digitales del comportamiento humano pueden permitir que los sistemas de IA infieran no solo las preferencias, la edad y el sexo de las personas, sino también su orientación sexual o sus opiniones religiosas o políticas. Para que las personas puedan confiar en el tratamiento de datos, debe garantizarse que tienen el pleno control sobre sus propios datos, y que los datos que les conciernen no se utilizarán para perjudicarles o discriminarlos”.

⁶⁶ En este sentido se expresa A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos...”, op. cit. pp. 45-46, quien acoge el término empleado en este discurso, “la gobernanza colectiva”.

⁶⁷ Esta nueva obligación ya ha sido advertida por autores como R. I. PALOMO VÉLEZ, *El modelo español de representación de los trabajadores en la empresa*, Tirant Lo Blanch, Valencia, 2017, p. 33

⁶⁸ Cfr. J.L. GOÑI SEIN, “Nuevas tecnologías digitales...”, op. cit. p. 5.

86. En el mismo orden, la norma estatutaria sigue el esquema clásico para regular el deber de sigilo y del secreto profesional enfocándolo a la protección de los intereses empresariales. Bajo la perspectiva examinada es necesario reconsiderar las funciones de éstos en cuanto al sigilo y al secreto profesional habida cuenta que la norma estatutaria los diseña con un estrecho margen de maniobra, un margen que no ha sido corregido en las sucesivas reformas que ha padecido la norma estatutaria.

87. Pues bien, planteamos un nuevo enfoque, totalmente novedoso y orientado a la funcionalidad y al alcance de un material especialmente sensible para proteger los derechos de los trabajadores afectados. En esta línea, se apuntó la propuesta de que el algoritmo debería ser conocido, su modelo y las variables de ponderación utilizadas, el tipo y las clases de datos que, a partir del modelo, se han suministrado para llegar al algoritmo.

88. Ahora bien, la controversia se suscita cuando este conocimiento de la propuesta de algoritmo (recuérdese que está diseñado por una persona) podría colisionar con los derechos de propiedad industrial, intelectual, y de forma concreta con el secreto empresarial. A pesar de esta colisión, compartimos que el conocimiento del algoritmo está totalmente justificado en los casos en los que éste pueda afectar a derechos fundamentales en el trabajo, en el acceso al empleo, en la igualdad o en la extinción del contrato de trabajo, de manera que una decisión de tal calibre no tendría que quedar a expensas de aquel.

89. Con ello se desea expresar que ante una vulneración de un derecho laboral se plantee la posibilidad de conocer el contenido del algoritmo (en los extremos expresados). Y sobre ello, la base de este planteamiento podría ser su posible impugnación y al derecho del trabajador afectado a una tutela judicial efectiva (artículo 24 de la Constitución Española). No obstante, queremos advertir que no es que haya que esperar a que se de una vulneración del derecho de protección de datos personales de un trabajador para que los representantes tengan que conocer los datos y el algoritmo, sino que debe deducirse ese conocimiento desde el momento en el que actúan y ejercen la defensa e intereses de los trabajadores. En este contexto, se abren un interrogante en relación a si es necesario que se recoja expresamente esta nueva competencia informativa o si sobre todo ante la ausencia de previsión normativa es factible argumentar que esa misma función representativa les otorga implícitamente.

90. Al respecto, se recuerda que los algoritmos (y la inteligencia artificial) no quedan exenta de sesgos, de errores ni de discriminaciones de los programadores a los que el legislador no puede permanecer inmune. En síntesis, y aunque no es preciso que se de una vulneración del derecho a la protección de datos, hay que entender que, si los derechos y los intereses de los trabajadores se pueden ver afectados, queda justificado el conocimiento de los datos y del algoritmo por parte de los representantes de los trabajadores dado que son ellos quienes ejercen la defensa de los derechos y de los intereses de aquellos.

91. Téngase en cuenta que, “solo conociendo el algoritmo y los datos concretos que se le han suministrado sobre la persona que propone la decisión podrían saberse las razones de la propuesta”, pues la tecnología no aporta valores que justifican de forma razonable y justificada esa decisión⁶⁹.

92. En definitiva, se aboga por “evitar sesgos del algoritmo que no puedan ser controlados por el interesado, precisamente por desconocer las razones por las que se ha tomado dicha decisión”. Con ello, se trata de evitar la indefensión “del sujeto al que le deniegan el empleo o le despiden en base a una decisión automatizada”⁷⁰.

⁶⁹ La posibilidad de conocer el algoritmo ante la vulneración de derechos fundamentales laborales ha sido ya planteada por T. DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, “Retos, Riesgos y Oportunidades de la Sociedad digital”, op. cit., pp. 47 y 48.

⁷⁰ Cfr. A. TODOLÍ SIGNES, “La gobernanza colectiva de la protección de datos...”, op. cit. pp. 80 y 81.

V. Conclusiones y propuestas de mejora

99. Una vez analizadas las consideraciones que han dado curso a la delimitación del objeto de estudio de esta materia proponemos como propuesta de mejoras:

100. Los dispositivos tecnológicos nacieron para atender las necesidades de los consumidores, pero no para ser empleados en el seno de las empresas con los propósitos detallados. A ello, se suma que a pesar del esfuerzo loable de la LOPD entendemos que resulta insuficiente en la regulación de la relación laboral española. Por ello, será clave, no solo una reforma laboral en clave digital que tenga en cuenta los derechos colectivos de los trabajadores, sino también, y más concretamente, la actuación de los interlocutores sociales a fin de que adopten fruto de la autonomía colectiva acuerdos que tutelen los derechos de los trabajadores afectados en la Era Digital.

101. La negociación colectiva debe enfocarse en acordar un tratamiento de datos justo con respecto al fin perseguido por la norma, que sea transparente al garantizar que los representantes de los trabajadores conozcan el algoritmo, y que no sea discriminatorio, que sea controlado por los representantes de los trabajadores.

102. Considerar que el tratamiento y la gestión de los datos que generan los dispositivos tecnológicos en el marco de las relaciones laborales forman parte del Derecho de información de los representantes legales de los trabajadores. De hecho, si el trabajador entiende vulnerado su derecho a la intimidad ha de presentar una prueba indiciaria que permita acreditar la estimación de los hechos que pretende probar. Ello podría justificar la entrega del algoritmo a los representantes de los trabajadores. Así, se plantea que dentro del derecho de información de los representantes legales de los trabajadores se disponga del algoritmo, pues podría ser un mecanismo probatorio en el proceso laboral. De hecho, la función de control y vigilancia del tratamiento de los datos personales de los representantes de los trabajadores se conjuga con el principio de responsabilidad activa exigido por la LOPD. Este principio exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pueda generar el tratamiento de datos de forma que los representantes puedan adoptar las medidas que procedan.

103. En relación con la aseveración anterior, no pretendemos ubicar el derecho de información de los representantes en modo defensivo, es decir, por la acción o permisión de un trabajador afectado, pues consideramos que el derecho de información de los representantes de los trabajadores es proactivo para defender los derechos de los trabajadores en general, en cuanto a la captación, gestión y tratamiento del empresario de los datos obtenidos de aquellos. En definitiva, justificamos la entrega del algoritmo en relación al fundamento y a la efectividad de la propia función representativa a cuyo servicio están los derechos de información de los representantes. No se le puede olvidar al lector que los derechos de información de los representantes de los trabajadores son derechos instrumentales para el ejercicio de su función representativa, y necesitaría el uso, el mal uso o indebido uso, es decir, si hay una gestión de los recursos humanos fraudulenta, los representantes pueden hacer uso de este algoritmo. Y ello, aunque en la actualidad no lo indique la norma, porque está justificado por el ejercicio de la función representativa. En otras palabras, el derecho de los representantes a conocer el algoritmo queda justificado en la medida en que ello es necesario para el ejercicio de sus funciones representativas y de defensa de los derechos de los trabajadores afectados.

104. Dada la amplitud del deber de confidencialidad y de secreto enunciado en la normativa de protección de datos, se podría entender aplicable a los representantes de los trabajadores, en el caso que éstos puedan tener acceso a esos datos. De forma concreta, los representantes de los trabajadores deben tener acceso al algoritmo empleado en el tratamiento de los datos de los trabajadores afectados por la decisión empresarial. Siempre que este principio quede sujeto en términos de secreto profesional reordenado para proteger a los trabajadores. En definitiva, el empresario no estaría facultado para negar el algoritmo a los representantes de los trabajadores porque entienda que es un secreto protegido. En este sentido, recuérdese que, en la Era Digital, el uso de algoritmos conduce a la creación de perfiles

como una información complementaria que tiene la empresa para la gestión del personal en momentos tan delicados como son el acceso al empleo, la clasificación profesional, la promoción profesional y los diversos elementos del poder de dirección y del poder disciplinario-sancionador. Así las cosas, los distintos dispositivos tecnológicos y los programas informáticos se han convertido en instrumentos de gestión e instrumentos de control para el ejercicio de un poder empresarial mucho más intenso y omnímodo. Teniendo en cuenta que el ejercicio de estos poderes, y el uso de estos algoritmos tienen riesgos para los intereses de los trabajadores (derechos fundamentales), y en aras de evitar el abuso y posibles situaciones discriminatorias, se apuesta por una acción preventiva, no defensiva, para intentar que el empresario en el ejercicio de esos derechos y esos poderes no lesione los intereses de los trabajadores. Unido a ello, se hace constar que, si el algoritmo es calificado como secreto empresarial, y sobre él pesa el deber de sigilo, consideramos que los representantes de los trabajadores no pueden utilizar el algoritmo más allá de su función representativa, es decir, esta información solo puede ser usada en el ejercicio de su función representativa, siendo éste el alcance del deber de sigilo impuesto. En este sentido, puede fundamentarse que el derecho de información se debe configurar como un elemento de protección del derecho a la intimidad de los trabajadores, pues los representantes son los veladores de estos datos, reforzándose de este modo el deber de sigilo.