

Prevención de riesgos laborales: marco legal y políticas gubernamentales relacionadas con las nuevas formas de trabajo en España, protección de los derechos a la seguridad y salud en el trabajo

Belén del Mar López Insua

**Profesora Titular de Derecho del Trabajo y de la Seguridad Social
Universidad de Granada**

blinsua@ugr.es

<https://orcid.org/0000-0002-1248-6015>

Resumen: El desarrollo de las tecnologías de la información y la comunicación ha supuesto un cambio en la forma de desarrollo de la prestación de servicios. Al tiempo que normativa laboral se ha ido tratando de adaptar a la realidad, aparecen nuevos riesgos necesitados de una protección específica. Por su parte, la normativa de seguridad y salud en el trabajo se ha visto abrumada y sobrepasada, en ciertos momentos, lo que ha exigido el desarrollo de tímidas normativas que completan a la Ley 31/1995 de Prevención de Riesgos Laborales. Por otro lado, el constante tira y afloja en sede judicial no ha hecho más que agravar los conflictos. Y es que, no siempre la jurisprudencia ha seguido una línea clara y garantista en pro de los derechos a la vida e integridad física y psíquica de los trabajadores. La falta de una negociación colectiva incisiva en la materia, por otro lado, no ha hecho más que agravar el problema. Quizás por la tecnicidad y especificidad de los problemas a tratar. Todos estos problemas, así como la falta de una verdadera cultura preventiva determinen que las empresas olviden y, lo que es peor, ignoren la normativa de prevención de riesgos laborales. Y es que, al hilo de las nuevas tecnologías emergen también nuevas formas de trabajo que precisan de una mayor protección y salvaguarda, sobre todo a fin de proteger los derechos fundamentales que les corresponden a todas las personas.

I. Las nuevas tecnologías a escena: perspectiva laboral y preventiva

Desde el surgimiento de la industrialización, las empresas han venido experimentando continuos cambios en los sistemas productivos que han afectado de lleno a las formas de gestión y organización de las relaciones laborales. El paso por diferentes modelos de desarrollo en el sistema económico evidencia un *modus operandi* común en todas estas transformaciones, en efecto, de lo que se trata es de adaptar las fuerzas de trabajo a las necesidades que en cada momento histórico reclama la sociedad¹.

La aparición de fórmulas jurídicas reguladoras de los posibles conflictos se ha mantenido en persistente mudanza desde que estalló la Revolución Industrial. Es por ello que, pese al paso del tiempo, continúen todavía hoy latentes las modificaciones del sistema normativo *iuslaboralista*. En fin, de lo que se trata es de adaptar la legislación a la realidad social presente. Sin embargo, este cometido no constituye tarea fácil, pues son a veces tan profundas las grietas que cuesta trabajo caminar en sintonía a los acontecimientos más recientes.

Asistimos actualmente a una auténtica «revolución» del mundo laboral motivado por la aparición de las recientes tecnologías de la información y comunicación (en adelante TIC) y su implantación en las empresas, lo que ha provocado un importante cambio de mentalidad y una transformación del derecho del trabajo². Rápidamente las TIC's van expandiéndose las redes de telecomunicaciones y, en especial, de Internet³, que si bien, aunque optimizan y agilizan enormemente el desempeño de la prestación profesional, permiten también almacenar información relativa a la persona del trabajador que se entremezcla a su vez con la actividad laboral⁴.

La progresiva informatización de muchas de las transacciones que diariamente son realizadas por las personas ha provocado que los trabajadores recurran a esta vía para realizar no sólo los quehaceres cotidianos de su vida laboral, sino también de su vida privada y personal⁵.

1 MERCADER UGUINA, J.R. «Derecho del Trabajo, nuevas tecnologías y sociedad de la información», Valladolid, Lex Nova, 2002, pág. 49.

2 SEMPERE NAVARRO, A. V Y SAN MARTÍN MAZZUCCONI, C. «Nuevas Tecnologías y Relaciones Laborales», Navarra, Aranzadi, 2002, pág. 31. SÁNCHEZ TORRES, E. «El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías», en *Relaciones Laborales y Nuevas Tecnologías*, obra colectiva dirigida por S. Del Rey Guanter y coordinada por M. Luque Parra, Madrid, La Ley, 2005, pág. 107.

3 LÓPEZ- BARAJAS PEREA, I. *La intervención de las comunicaciones electrónicas*, Madrid, La Ley, 2011, pág. 21.

4 SEGOVIANO ASTABURUAGA, M.L. «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», en *Revista Jurídica de Castilla y León*, n.º 2, febrero de 2004, pág. 149.

5 SÁNCHEZ TORRES, E. «El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías», en *Relaciones Laborales y Nuevas Tecnologías*, obra colectiva dirigida por S. Del Rey Guanter y coordinada por M. Luque Parra, Madrid, La Ley, 2005, pág.108.

Lo cual abre las puertas a los empresarios a que sospechen, ante el miedo por una posible caída de la actividad productiva, del uso diligente y proporcionado que sus trabajadores hacen de los medios digitales.

La generalización de este fenómeno se ha extendido más allá de lo imaginable, en comparación con lo que sucedía hace escasos años atrás. Es por ello que muchas empresas han optado por controlar todos los períodos que componen este proceso, es decir, no sólo los resultantes de una determinada actividad profesional, sino también aquellos que componen o forman parte de la *privacy* de toda persona. De ahí que, hoy día, la doctrina utilice el término «trabajador transparente» o «trabajador de cristal» para hacer referencia a los inminentes mecanismos de control empresarial tanto laboral como extralaboral que son dispuestas por las empresas⁶.

Con la llegada de la cuarta revolución industrial o industria 4.0 se suman nuevas injerencias y retos que ponen, en tela de duda, el derecho a la intimidad de los trabajadores. Y todo ello, con motivo de la digitalización de la industria y del desempeño de la actividad profesional. En efecto, con la entrada de esta cuarta revolución industrial se produce una nueva organización de los modelos de producción, lo que supone una irrupción en los sistemas de producción de las nuevas TICs para así incrementar la productividad, al tiempo que disminuye el número de trabajos manuales y se incrementan, por contra, los trabajos de dirección y de gestión empresarial. Ello determina una flexibilización del tiempo y lugar de trabajo para así facilitar la interacción directa entre el cliente y el trabajador. Lo que, asimismo, genera un importante flujo y volumen de datos para su agrupamiento, almacenamiento y análisis⁷.

Entre las principales tecnologías implicadas en la digitalización de las empresas cabe destacar: *Big data*; *Blockchain* o cadena de bloqueo; *Cloud computing* o computación en la nube; Fabricación aditiva o fabricación por adición; Impresión 3D; Inteligencia artificial; Realidad aumentada; Realidad virtual; Ciberseguridad o seguridad en la red; 5G; Robots y robots colaborativos; las redes sociales; los nuevos sistemas de geolocalización y el denominado Internet de las cosas (IoT).

Precisamente, es en este punto en donde se ha planteado una fuerte tensión dialéctica entre dos derechos que disfrutan de una dimensión constitucional diferente, de un lado, la propiedad privada y la tutela del patrimonio empresarial (artículo 38 de la Constitución Española —CE—) y, de otro lado, los derechos fundamentales (Capítulo II, sección 1.ª de la CE) a la intimidad (artículo 18.1 de la CE), al secreto de las comunicaciones (artículo 18.3 de la CE), a la dignidad (artículo 10.1 de la CE) y a la libertad de expresión (artículo 20.1 de la CE). Se han suscitado multitud de cuestiones en torno a este tema, pero, sin duda, el más conflictivo ha sido el de determinar el alcance de cada uno de los derechos, así como los límites que podrán imponerse por el acreedor de la prestación de trabajo⁸.

6 SEGOVIANO ASTABURUAGA, M.L. «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», en *Revista Jurídica de Castilla y León*, n.º 2, febrero de 2004, pág. 149.

7 FERNÁNDEZ COLLADOS, M.B. «El uso de las nuevas tecnologías en las relaciones laborales. Propuestas y soluciones ante nuevos retos y viejos conflictos», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, N.º 57, 2020, págs. 324-325.

8 LÓPEZ INSUA, B.M. «Derecho fundamental a la intimidad del trabajador y poderes empresariales», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 38, julio de 2014.

El vigente 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 (ET) no podía ni tan siquiera presentir, en el momento de su nacimiento, el vertiginoso avance que han experimentado las TIC. Y es que pese al sinfín de reformas y contrarreformas que ha sufrido la legislación vigente en España, el legislador no ha sabido todavía dar respuesta a un problema que cada vez está más patente en la práctica diaria de las empresas⁹. La falta de una concreta regulación ha hecho estragos en el panorama social, creando además un enfrentamiento entre derechos de distintos rango que no debería coexistir, pues como bien dijo el Alto Tribunal allá por el año 1981: «Tampoco puede aceptarse la tesis... de que los derechos reconocidos o consagrados por la Constitución sólo pueden quedar acotados en virtud de límites de la propia Constitución o por la necesaria acomodación con el ejercicio de otros derechos reconocidos y declarados igualmente por la norma fundamental» (STC 11/1981, de 8 de abril de 1981 (BOE número 99 de 25 de abril de 1981) en su fundamento de derecho número 7). Por lo que no cabe imponer ningún límite al ejercicio de los derechos fundamentales, ni tan siquiera mediante la puesta en marcha de otros derechos u otras formas de control en virtud del poder de dirección que le corresponde al empresario¹⁰. En este sentido, los tribunales vienen señalando que la limitación de los derechos fundamentales del trabajador como consecuencia del poder empresarial de control y dirección solo puede derivarse de que la propia prestación y naturaleza del servicio implique esta restricción. Por lo que, en todo caso, la medida adoptada por la parte empresarial deberá respetar el principio de proporcionalidad, atendiendo a la idoneidad de la medida para la consecución del objetivo propuesto; la necesidad de la misma, en tanto que no exista otra medida destinada al mismo fin y la proporcionalidad estricta, en tanto que la medida adoptada deberá ser equilibrada en relación al fin perseguido¹¹.

Quizás, por ello, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y Garantía de los Derechos Digitales haya incluido, en su Disposición Final Decimotercera un artículo 20 bis al ET, en donde se indica 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 digitales».

El legislador estatutario no ha creado un marco legal de referencia para la defensa de la *privacy* del trabajador, a diferencia de lo que sucede en otros ordenamientos jurídicos europeos en los que sí se tiene madurada una idea de protección de la esfera privada del trabajador¹². Efectivamente, en nuestro caso el Constitucional se ha limitado a devaluar el contenido mismo de este derecho al enunciar más una propuesta programática que hacer efectivo su tutela¹³. De ahí que la solución al problema radique en la judicialización de los conflictos, pero no sólo a nivel nacional, sino también elevados a rango comunitario e internacional. Pues la protección de la intimidad en particular y de los derechos fundamentales en general constituye no sólo una

9 GÓMEZ SANCHIDRIAN, D. «Las nuevas tecnologías en las relaciones laborales: Control empresarial del correo electrónico y de Internet», en *Noticias Jurídicas*, noviembre de 2012, pág. 1.

10 GOÑI SEIN, J.L. «El respeto a la esfera privada del trabajador», Madrid, Civitas, 1988, págs. 21-31.

11 MONEREO PÉREZ, J.L. Y LÓPEZ INSUA, B.M. «El control empresarial del correo electrónico tras la STC 170/2013», *Aranzadi Social- Revista Doctrinal*, Número 11, marzo de 2014, pág. 240.

12 RAPP, L. «Secret de correspondances et courriers électroniques», *Dalloz*, n.º 41, 2000, págs. 3 a 5.

13 GOÑI SEIN, J.L. «El respeto a la esfera privada del trabajador... op.cit., págs. 28-29.

exigencia de carácter político, sino lo que es aún mejor, una garantía y compromiso que habrán de superar todos los Estados que forman parte de la Unión Europea —UE—¹⁴.

Fundamentalmente, la penetración y protección de los derechos fundamentales en el ordenamiento comunitario se ha debido a la decidida intervención del Tribunal de Justicia de la Unión Europea (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH). Ambos se han erigido en los máximos exponentes y responsables (sobre todo el TEDH) de la salvaguardia de dichos derechos para el Colectivo Europeo. Es por ello por lo que, a la hora de fijar los límites, alcance y contenido de cada uno de éstos, se haya de tener en cuenta no sólo lo dispuesto por la normativa común, sino también por la Norma Madre de cada uno de los Estados miembros. Muy acertadamente señala a el Tribunal de Justicia de la Comunidad Europea, en su sentencia de 14 de mayo de 1974 (Asunto 4/73), que: «... los derechos fundamentales forman parte de los principios generales del derecho que debe respetar... (el propio Tribunal) ... Al velar por la protección de tales derechos este Tribunal se basa en la tradición constitucional común a los Estados miembros, de manera que no puede permitir medidas incompatibles con los derechos fundamentales reconocidos y garantizados por las Constituciones de los Estados miembros».

En este contexto jurídico se han adoptado una serie de instrumentos normativos que tratan de mantener unas garantías mínimas que aseguren el pleno respeto a los derechos y libertades fundamentales. En este sentido, a nivel comunitario destacan, de un lado, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) firmado en Roma el 4 de noviembre de 1950 y de otro lado, la Carta de los Derechos Fundamentales de la UE -2000/C 364/01- (CDFUE). Entre las Directivas europeas cabe citar: la 95/46 CE del Parlamento Europeo (PE) y del Consejo de 24 del 10 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; la 97/66 CE de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y la 2002/58 CE del PE y del Consejo de 12 de julio del 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Y con vocación de universalidad llaman poderosamente la atención: el Pacto Internacional de Derechos Civiles y Políticos, ratificado por la Asamblea General de la ONU en su resolución 2200 A (XXI), de 16 de diciembre de 1966 y la Declaración Universal de Derechos Humanos, proclamada también por la Asamblea General en su Resolución 217 A (III) de 10 de diciembre de 1984.

II. Las nuevas formas de trabajo: plataformas digitales y problemas prácticos

La industria 4.0 o también conocida como Cuarta Revolución Industrial no sólo implica a sistemas inteligentes o conectados, sino que su alcance es aún más amplio en tanto que abarca también a la nanotecnología y a las energías renovables. Consiste, por tanto, en la fusión de esas tecnologías y su interacción, en el ámbito profesional, con los dominios físi-

14 RODRÍGUEZ LAINZ, J.L. «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: derecho primario», en *Diario La Ley*, núm. 7351, 2010, pág. 2.

cos, digitales y biológicos. Ello determina que esta Cuarta Revolución Industrial sea diferente a las anteriores. En efecto, mientras que la Primera Revolución Industrial supuso la aplicación del vapor a la producción mecánica (llega sobre el año 1784); la Segunda Revolución Industrial introdujo la producción masiva basada en la electricidad y la producción en cadena (se sitúa entre finales del siglo XIX y principios del XX) Por su parte, la Tercera Revolución Industrial fusiona las tecnologías de la comunicación con la programación de las máquinas, el uso del internet y las tecnologías renovables (se desarrolla entre 1969 y finales del siglo XX) y, finalmente, con la Cuarta Revolución Industrial surgen las fábricas inteligentes y la gestión online de la producción.

En este marco surgen, como una nueva forma de negocio, las plataformas digitales. Lo que determina que, cada vez más, los usuarios o clientes acudan a páginas webs o apps para recibir cualquier servicio. Hacen su entrada estelar, en este punto, plataformas digitales como: *Uber, Stuart, Airbnb, Booking, TripAdvisor, BlaBlaCar, Glovo, Deliveroo, HBO, Netflix, Amazon...* etcétera. Poco a poco, la compra y venta online se va popularizando, de forma que la inteligencia humana comienza a sustituirse —aunque lentamente— por el *lot*, la domótica, la robótica..., incluso ya a través del *big data* se puede realizar el análisis de grandes datos. La inteligencia artificial está, por ejemplo, reemplazando a los humanos en algunas actividades de traducción de idiomas, conducción o ventas minoristas. De ahí que, algunos autores, teman ante una posible huída del Derecho del Trabajo¹⁵, debido a la aparición de las nuevas tecnologías. De igual modo, las *startups* y la economía colaborativa o el *crowdsourcing*... avanzan a pasos agigantados con el propósito de formar parte de la cotidianeidad de gran parte de la población, extendiéndose la utilización de todo tipo de plataformas digitales.

Aunque las repercusiones de este gran fenómeno son aún impredecibles, está claro que la economía de las plataformas paulatinamente se ha ido asentando en el panorama laboral llegando, incluso, a cuestionar la misma noción de trabajo por cuenta ajena¹⁶. Como en toda revolución tecnológica, la Industria 4.0 ha provocado una destrucción de empleos¹⁷, a la par de un surgimiento de nuevas oportunidades de negocio antes insospechadas, siendo un claro ejemplo de nuestros tiempos el de las *youtubers* e *influencers* auspiciados al fragor de las redes sociales¹⁸.

El modelo de negocios de las *startups* se ha asentado en sectores tradicionales de actividad sólidamente consolidados (a saber: restauración, viajes, televisión, transporte...), lo que ha determinado una radical transformación en sus formas y modos de desempeño de la actividad profesional. Justo, en este contexto, se implantan los dispositivos de geolocalización

15 En *Derechos Laborales fundamentales inespecíficos*, obra colectiva dirigida por José L. Monereo Pérez, Francisco Vila Tierno y Juan C. Álvarez Cortés y coordinada por Belén del M. López Insua, Granada, Comares, 2020.

16 López Insua, B.M. «Trabajo decente y prestaciones ante situaciones de necesidad (I): Incapacidad para trabajar», en *El trabajo decente*, obra colectiva dirigida por José L. Monereo Pérez, Juan Gorelli Hernández y Ángel L. De Val Tena y coordinada por Belén del M. López Insua, Granada, Comares. Colección Trabajo y Seguridad Social n.º111, 2018.

17 RODRÍGUEZ ESCANCIANO, S. Y ÁLVAREZ CUESTA, H. *Trabajo autónomo y trabajo por cuenta ajena: nuevas formas de precariedad laboral*, Bomarzo, 2019.

18 FERNÁNDEZ COLLADOS, M.B. «El uso de las nuevas tecnologías en las relaciones laborales. Propuestas y soluciones ante nuevos retos y viejos conflictos», *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm.57, 2020, pág. 326.

en los equipos de trabajo que son facilitados por las empresas. Lo que provoca un aumento del control empresarial en la prestación de servicios de sus trabajadores, al tiempo que una posible vulneración del derecho fundamental a la intimidad y a la dignidad de los trabajadores¹⁹ que son expuestos a dichos dispositivos²⁰.

A raíz de la introducción de esta Cuarta Revolución Industrial se produce un cambio o transformación no sólo en el modelo de producción, sino también en las relaciones entre la empresa y sus clientes y, por ende, en el concepto de Derecho del Trabajo²¹. Ciertamente, aunque no se produzca aún el fin del trabajo, lo que si se pronostica es una modificación en los contratos de trabajo y una viralización de las condiciones de trabajo²². Lo que, irremediablemente, provocará un efecto negativo sobre los derechos de los trabajadores²³.

Pueden resumirse algunas de las características de estas plataformas digitales en las siguientes: 1) la organización y atribución de tareas a través de algoritmos; 2) transparencia; y 3) cierta autonomía y no exclusividad. Conviene precisar ese concepto de «algoritmo», mencionado en el primer punto, para entender este tipo de relaciones. De acuerdo, con la ley de propiedad intelectual los derechos de explotación de los algoritmos realizados en el ámbito de una relación laboral se asignan al empresario. No obstante, se diferencian entre dos supuestos. Por una parte, cuando se realizan fruto de la actividad habitual del trabajador y, por otra, cuando el algoritmo se realiza fuera de las funciones normales del trabajador.

Respecto al primer supuesto, la regulación atribuye sin más al empresario los resultados del trabajo del asalariado. Cuestión lógica derivada de que al trabajador se le contrató precisamente para que realizara ese algoritmo, por lo que no cabe duda de que el salario del trabajador es justificación suficiente para que el empresario se apropie del resultado del trabajo. En el segundo supuesto, en caso creación de un algoritmo *fuera de las funciones habituales del trabajador*, el empresario *ex-lege* se apropia de los derechos de explotación del programa de ordenador creado por el trabajador sin tener que pagar compensación alguna.

De acuerdo con estas ideas, el algoritmo será el empresario, es decir, quien organiza y planifica la actividad, asignando las tareas al profesional que –en cada momento concreto– que reúna los requerimientos profesionales y geográficos más aptos para cubrir las necesidades del cliente. Principalmente, estas labores son las que realizan los *riders*. Colectivo, sobre el cual, se ha generado todo un intenso debate jurisprudencial en torno a la determinación de las notas de laboralidad y ajeneidad de los servicios que prestan a través de las plataformas digitales. Y es que, en teoría, quien presta dichos servicios puede rechazarlo y no tiene exclusividad con la empresa²⁴. Empero, todo ese debate doctrinal y jurisprudencial ha quedado zan-

19 MONEREO PÉREZ, J.L. *La dignidad del trabajador. Dignidad de la persona en el sistema de Relaciones Laborales*, Murcia, Laborum, 2020.

20 MARÍN MALO, M: «La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente», en *Labos*, Vol.1, núm.1, 2020, pág. 111.

21 MERCADER UGUINA, J. R. «El futuro del trabajo en la era de la digitalización y la robótica», Valencia, Tirant lo Blanch, 2017, pág. 613.

22 RODRÍGUEZ ESCANCIANO, S. Y ÁLVAREZ CUESTA, H. «Trabajo autónomo y trabajo por cuenta ajena: nuevas formas de precariedad laboral», Bomarzo, 2019.

23 En *El impacto de la industria 4.0 en el trabajo: una visión interdisciplinaria*, obra colectiva dirigida por Djamil Kahale Carrillo, Navarra, Aranzadi, 2020.

24 MONEREO PÉREZ, J.L. Y LÓPEZ INSUA, B.M. «Las difusas fronteras entre el trabajo asalariado y por

jado tras la sentencia del Tribunal Supremo de 25 de septiembre de 2020 (núm. 805/2020) y, el posterior, Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales (BOE núm. 113 de 12 de mayo de 2021). Así es, por un lado, en el fallo del Tribunal Supremo se resuelve a favor de la laboralidad de las prestaciones de servicios en plataformas digitales de reparto. Siendo así, ésta, la primera sentencia dictada en unificación de doctrina que, valiéndose de la prevalencia del principio de realidad en el sentido señalado por sentencias precedentes como las de 26 de febrero de 1986 o de 20 de enero de 2015, resalta la necesidad de adaptar los requisitos de dependencia y ajenidad al contexto actual. Por otro lado, el Real Decreto-ley 9/2021 reproduce los mismos criterios y parámetros establecidos por el Tribunal Supremo y, para ello, introduce en el ET una nueva disposición adicional 23.^a. En particular, esta disposición presume ahora la laboralidad en el ámbito de las plataformas de reparto: «Por aplicación de lo establecido en el artículo 8.1, se presume incluida en el ámbito de esta ley la actividad de las personas que presten servicios retribuidos consistentes en el reparto o distribución de cualquier producto de consumo o mercancía, por parte de empleadoras que ejercen las facultades empresariales de organización, dirección y control de forma directa, indirecta o implícita, mediante la gestión algorítmica del servicio o de las condiciones de trabajo, a través de una plataforma digital».

A pesar de los avances y de la lucha por la laboralización de los *riders*, lo cierto es que todavía queda mucho camino por avanzar. La protección de los derechos de los trabajadores debe convertirse en una prioridad y, para ello, la normativa laboral y de Seguridad Social debe adaptarse. Es por ello que se reclame el establecimiento de un nuevo y específico marco jurídico para estas actividades que adapte no sólo este tipo de relaciones al modelo contemporáneo que reclama el Derecho del Trabajo²⁵, sino que además implique a los representantes de los trabajadores.

III. Derechos fundamentales y control empresarial: de la ficción a la realidad

El funcionamiento de los algoritmos, a través de la inteligencia artificial, permite poner en marcha un mecanismo que se mueve entre la lógica humana y la lógica de traducción y que aspira programar tareas que un ordenador o, en general, las TIC son capaces de procesar²⁶. A

cuenta propia. *Riders y plataformas digitales de nuevo a examen en la doctrina de los Tribunales Superiores de Justicia. STSJ de Madrid-SOC núm. 40/2020, de 17 de enero*», en *Anuario de 2020 de Jurisprudencia Laboral (Estudio de 100 casos relevantes)*, Madrid, BOE, 2021, págs. 415-430.

25 MONEREO PÉREZ, J.L. Y LÓPEZ INSUA, B.M. «Las difusas fronteras entre el trabajo asalariado y por cuenta propia. *Riders y plataformas digitales de nuevo a examen en la doctrina de los Tribunales Superiores de Justicia. STSJ de Madrid-SOC núm. 40/2020, de 17 de enero*», en *Anuario de 2020 de Jurisprudencia Laboral (Estudio de 100 casos relevantes)*, Madrid, BOE, 2021, págs. 415-430.

26 COMMATTEO, G Y MOREYRA, P. «Discriminación 4.0: una aproximación a los problemas que suscitan la biométrica y los sistemas de reconocimiento facial», en *Revista Internacional de Derechos Humanos*, Vol. 2, N.º 1, 2022, pág. 20.

este respecto, la inteligencia artificial sirve a la biométrica al objeto de establecer entornos de interacción inteligente que perciban rasgos, datos y emociones del usuario.

El término «biometría» viene referido a todos aquellos «... métodos automatizados de verificación o reconocimiento de identidad de una persona con vida basado en características físicas o contractuales»²⁷. De manera inequívoca, el «Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta a tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE» (en adelante RGPD) define en su artículo 4 los datos biométricos como aquellos «datos personales obtenido a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identidad única de dicha persona, como imágenes faciales o datos dactiloscópicos». A buen ejemplo, la forma en que desbloqueamos los teléfonos móviles a partir del reconocimiento facial o la huella dactilar, constituye una forma de biométrica. Las tecnologías biométricas no determinan la verdadera identidad de la persona, sino que se enfocan en vincular patrones a atributos personales.

En función de la naturaleza, aparecen tres tipos de datos biométricos: a) el universal, se tratan de datos que se dan en todas las personas; b) el único, aparece cuando se distingue en cada persona y c) el permanente, cuando se mantenga a lo largo del tiempo. En este sentido, encontramos diferentes tipos de características biométricas y que pueden dividirse en características biológicas (a saber: cara, mano, retina, iris, huellas dactilares, vasculares... etcétera) y de comportamiento (firma, tipificación, voz o la forma de andar de la persona). Aparte de estos datos biométricos, con el paso del tiempo han ido apareciendo otros, a saber: el estudio de la palma de la mano, la forma de las orejas, el ADN, la piel... etcétera.

En relación a la finalidad del tratamiento, las operaciones con datos biométricos tienen por objetivo: 1) la detección de seres humanos; 2) la detección de un rostro u otra particularidad anatómica; 3) evaluación de modelos y comportamientos; 4) perfilado, clasificación y toma de decisiones; 5) autenticación; 6) identificación y 7) seguimiento de individuos.

En el ámbito de las relaciones empresariales, entidades como Google, Facebook, Amazon, Spotify, Airbnb, Uber, Tesco, Apple... etcétera, usan los algoritmos en el día a día de sus quehaceres cotidianos y, también, en el ámbito de las relaciones con sus trabajadores y los usuarios. Llama poderosamente la atención, a este respecto, el caso que saltó en el año 2018 de Amazon. Y es que la empresa, para ahorrar costes de personal, decidió despedir a sus empleados para sustituirlos por la inteligencia artificial. Amazon, ambiciosamente, aspiraba a lograr una mayor productividad y ahorro de tiempo mediante el uso de un nuevo sistema —teóricamente «neutral»— que seleccionara y contratara al personal, entendiendo —por otro lado— que la mirada humana resulta siempre parcial o llena de sesgos que muchas veces son inconscientes y/o difíciles de superar. Este sistema de inteligencia artificial se entrenó sobre la base de información que le proporcionaba el *Big Data* y que se circunscribía a recoger los datos de los solicitantes de empleo en Amazon durante un período de diez años. Este mecanismo fue entrenado para observar patrones. Ahora bien, vino la gran sorpresa cuando la empresa tuvo que «despedir» a su «nuevo reclutador», artificial y supuestamente neutral porque provocó una enorme discriminación por razón de sexo. Aunque resulte paradójico, el

27 ESCAJEDO SAN EPIFANIO, L. «Reconocimiento e identificación de las personas mediante Biométricas estáticas y dinámicas», *Tesis Doctoral de la Universidad de Alicante*, 2015.

algoritmo a través del cual funciona este «nuevo reclutador», arrojaba resultados con una preferencia por candidatos masculinos, dado que los reclutamientos anteriores y los *curriculum vitae* oportunamente enviados a la empresa provenían, en su gran mayoría, de hombres, lo que evidencia un reflejo del dominio masculinizado de la industria tecnológica²⁸.

Junto a los datos biométricos hay que considerar el *Big Data*, el cual se sirve —entre otros— de los buscadores o redes sociales para recolectar y analizar datos de usuarios. Cuanta más información proporcione un usuario, mayor serán las ofertas especializadas de productos y servicios que se le pueden ofrecer. De este modo, los usuarios son agrupados por sus intereses y, en base a ello, están expuestos a ciertas publicidades online, pero también a ciertas ofertas de empleo (en el caso de que se busque trabajo). Un problema que genera la publicidad personalizada es que los usuarios quedan aislados en «burbujas digitales» o «burbujas de publicidad digital». Además, las compañías ocultan las categorías en las que agrupan a los usuarios, por lo que, al final, los propios usuarios no saben si están siendo catalogados de un modo o de otro²⁹.

Cabe citar aquí el caso Facebook que saltó a la palestra en el año 2019. La mencionada empresa inició el desafío denominado «Ten year challenge» que, en realidad, ocultaba un mecanismo de control biométrico. En concreto, este desafío solicitaba a los usuarios que subieran una foto actual y otra de 10 años de antigüedad, en principio, sólo por «diversión». Sin embargo, lo que se convirtió rápidamente en una tendencia, presuntamente indefensa, fue posteriormente cuestionada por muchos usuarios: ¿realmente no sería un mecanismo para que Facebook aglutinara datos de personas provenientes de todo el mundo? Se piensa que, esos datos sobre los rasgos faciales de todas esas personas de distintas edades, podrían emplearse para entrenar algoritmos que se apliquen durante un proceso de reconocimiento fácil.

Ya algunas películas, como «Minority Report», la «Guerra de las Galaxias», «Regreso al futuro», «Star Trek» o «Iron Man» predijeron el impacto que el uso de reconocimiento facial iba a tener en la sociedad, pero también en el ámbito de las relaciones laborales (como en la película «Misión imposible»).

A día de hoy, los datos biométricos sirven para diferentes funciones. Entre los usos más habituales encontramos la protección de identidad del usuario, puesto que se pueden emplear, a través de tecnologías de escáner y reconocimiento, para autenticar y verificar la identidad de una persona. También se emplean como método de control de acceso a instalaciones; en vez de usar tarjetas, se usa un lector de huellas (es el más habitual) para autorizar el acceso de las personas cuya huella figura en la base de datos. Incluso, en los aeropuertos no es raro recurrir a la anatomía particular de los pabellones auditivos para identificar a individuos que se muestran difíciles de reconocer usando métodos de reconocimiento facial habituales, al engañar al sistema usando barbas, bigotes esposos, gafas, pelucas, cambios de coloración del cabello o, incluso, las mascarillas durante la pandemia del COVID-19. Su estudio concreto

28 Dastin, 10 de octubre de 2018, «Amazon scraps secret AI recruiting tool that showed bias against women», Véase: <https://www.reuters.com/article/us-amazon-comjobs-automation-insight-idUSKCN1MK08G>

29 COMMATTEO, G Y MOREYRA, P. «Discriminación 4.0: una aproximación a los problemas que suscitan la biométrica y los sistemas de reconocimiento facial» ... op.cit., págs. 29 y 30.

y de representación bidimensional del pabellón es característica de cada individuo y de su estado concreto de desarrollo en la ontogenia, se trata del otograma³⁰.

Otro de los usos habituales es el control de migración o aduanas; los pasaportes biométricos llevan varios años usándose en diferentes países. En su chip almacenan los datos biométricos del titular, junto a otros datos personales, lo que permite un control más ágil y rápido.

Cada vez más, se utilizan los distintos mecanismos biométricos de los trabajadores para controlar el uso diligente y proporcionado de las relaciones de trabajo, incluso para verificar el cumplimiento de los parámetros pactados. En el marco de un tratamiento digno, sea cual sea la técnica biométrica empleada, lo cierto es que se vigilará que ésta cumpla con los criterios de adecuación, proporcionalidad y necesidad. Tanto la finalidad de la medida, como el impacto que pueda tener sobre los derechos y libertades de las personas físicas conlleva una serie de riesgos tanto para el individuo, como para la sociedad.

El «Big Data» o la acumulación de datos masivos. En concreto, la expresión «Big Data» aparece referido al volumen, esto es, a la cantidad de datos —casi inabarcable en la mente humana— que son creados por los humanos y que permiten realizar transacciones o buscar en webs y redes sociales. Los datos masivos se generan durante la navegación por internet, las comunicaciones del internet de las cosas, comunicaciones entre máquinas, industrias, estaciones meteorológicas... etcétera, por lo general vinculadas a medidores y sensores de temperatura, luz, altura, presión, sonido, localización, GPS, así como en el entorno de tecnologías RFID, wifi o bluetooth. A sumar a los datos biométricos, normalmente vinculados al ámbito de seguridad, pero también de sanidad (escáneres de retina, de huellas digitales, o lectores de cadenas de ADN, monitoreos médicos de todo tipo, etcétera)³¹.

El uso desviado tanto de los datos biométricos, como del «Big Data» incide no sólo el respecto al derecho a la dignidad de las personas (artículo 10.1 de la CE) y la protección de datos³², sino también en otros derechos fundamentales como: la intimidad, la igualdad, el honor, la propia imagen y la integridad (física y psíquica).

A nivel europeo existe una gran preocupación sobre esta materia. Por esta razón, el Reglamento General de Protección de Datos³³ indica que, a la hora de evaluar y determinar el riesgo

30 PRIYADHARSHINI, R.A., ARIVAZHAGAN, S Y ARUN, M. «A deep learning approach for person identification using ear biometrics», en *Appl Intell (Dord)*, 51(4), 2021, págs. 2161 a 2172.

31 COTINO HUESO, L. «Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales», en *DILEMATA*, año 9, núm. 24, 2017, pág. 133.

32 A este respecto, a fecha de 23 de junio de 2020, la Agencia Española de Protección de Datos (AEPD) ha publicado una «nota técnica» que incluye catorce equívocos relacionados con el uso de la biométrica y la protección de datos. El documento dirigido a empresas, encargados, Delegados de Protección de Datos...etcétera, tiene por objeto ofrecer una información acerca de las confusiones e imprecisiones más comunes que suelen asociarse al uso de esta tecnología informática. Entre los equívocos más comunes se encuentra la afirmación de que los sistemas de identificación y autenticación biométrica son más seguros para los usuarios. En este sentido, se advierte que el acceso no autorizado a los datos biométricos en un sistema permite o facilita el acceso al resto de sistemas que utilizan datos biométricos. Ver: <https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf>

33 Diario Oficial de la UE de 4 de mayo de 2016 (L 119/1).

para los derechos y libertades de los individuos en el procesamiento de los datos, se habrá de emplear criterios de clasificación de las operaciones biométricas tomando como punto de referencia la ley de protección de datos, con relación al tratamiento en el que se implementan.

En concreto, el Reglamento europeo para la protección de datos apuesta por mecanismos proactivos y preventivos en vez de reactivos, que precisamente tienen especial importancia para el «Big Data» y los mecanismos biométricos. Por este motivo, el artículo 25 del Reglamento europeo, impone la protección de datos desde el diseño y por defecto, de modo que la privacidad se integre desde el inicio en la gestión y ciclo de vida del tratamiento de datos. Y, lo mismo, debe aplicarse respecto del derecho a la no discriminación, hay que integrar la no discriminación con estas medidas preventivas. En concreto, el Reglamento europeo de protección de datos exige que, antes de adoptar una medida, las empresas lleven a cabo una Evaluación de impacto de protección de datos (artículo 35 Reglamento). Y, precisamente, los usos del «Big Data» y los datos biométricos son claros candidatos a que dicha evaluación de impacto sea obligatoria, por cuanto suelen suponer la elaboración de perfiles y porque sobre el resultado del tratamiento se basan decisiones que produce efectos jurídicos sobre el individuo, o que pueden afectar de manera significativa a los individuos (artículo 35.3.º del Reglamento europeo). Hay que apostar en ir más allá de la protección de datos e integrar en estas medidas preventivas para evitar la discriminación.

Evidentemente, este tipo de garantías para los trabajadores frente a las posibles violaciones de derechos habrán de combinarse con el reconocimiento de fuertes facultades de acceso y conocimiento de los algoritmos y los grandes datos que se manejan por parte de sectores especializados, tanto públicos como privados. Y dicha transparencia ha de venir acompañada, asimismo, con el reconocimiento de fuertes potestades de control respecto de los *data brokers* que son claves en el sector. Sin perjuicio del control que pudieran efectuar los agentes sociales y representantes de los trabajadores, el poder judicial habrá de examinar —en último lugar— la proporcionalidad de las medidas adoptadas para el fin que se pretende conseguir.

3.1. El Derecho a la intimidad versus la fijación de un juicio de proporcionalidad

Nuestra Carta Magna protege al máximo nivel de garantías los derechos reconocidos en el Capítulo II, sección 1ª de la CE, intitulado «De los derechos fundamentales y de las libertades públicas». Ello significa que sólo por Ley Orgánica se podrá desarrollar su contenido (artículo 81 CE), siendo éstos objeto de la protección reforzada que establece el artículo 53.2 de la vigente Constitución Española (CE): «Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en... la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional...».

La jurisprudencia insiste en que el derecho a la intimidad busca proteger un mismo objetivo, esto es, la esfera privada de las personas frente a las intromisiones que pudieran producirse por parte de terceros ajenos a la misma³⁴. Por lo que de acuerdo con esta idea, los derechos funda-

34 MARTÍN MORALES, R. «El régimen constitucional del secreto de las comunicaciones», Prólogo a la obra cargo de Francisco Balaguer Callejón, Madrid, Civitas, 1995, pág. 13. ROMERO PÉREZ, X.L. «El

mentales que son reconocidos por nuestra CE no podrán quedar suspendidos por el hecho de que exista una relación laboral: «la celebración de un contrato de trabajo no implica, en modo alguno, la privación de derechos fundamentales para quienes prestan servicio en las organizaciones productivas, que son ajenas a los principios y derechos constitucionales que informan el sistema de relaciones de trabajo... (sentencias del Tribunal Constitucional (TC): 197/1998, de 13 de octubre (RTC 1998, 197) y 98/2000, de 10 de abril (RTC 2000, 98). Ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad, ni la libertad de empresa, que establece el artículo 38 CE legitima el que quienes prestan servicios en aquéllas por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional. Las manifestaciones de «feudalismo industrial» repugnan al Estado social y democrático de Derecho y a los valores superiores de libertad, justicia e igualdad a través de los cuales ese Estado toma forma y se realiza (sentencias del TC 88/1985, de 19 de julio de 1985 (BOE núm. 194, de 14 de septiembre) y 170/2013, de 7 de octubre del 2013 (BOE de 7 de noviembre de 2013))»³⁵.

Ahora bien, como ya se ha puesto de manifiesto, existe también un poder de dirección del empresario que en ocasiones interfiere en la esfera de los derechos inherentes al trabajador. La cuestión es ¿hasta dónde puede llegar esa potestad empresarial a controlar el ejercicio de determinados derechos fundamentales? Constituye éste un asunto peliagudo que ya ha sido objeto de análisis por nuestros tribunales (nacionales y europeos) en varias ocasiones, pero que sin embargo no ha logrado todavía implantar una doctrina consolidada y definitiva enfocada hacia una protección universal de los derechos fundamentales. Las constantes contradicciones jurisprudenciales son muestra evidente de esa falta de tradición jurídica en nuestro país de la problemática de la *privacy* del trabajador y de la ausencia de un marco legal de referencia en el vigente ET.

La intimidad se configura como un derecho fundamental de carácter subjetivo³⁶ que no se define ni por la propia CE ni tampoco por la LO 1/1982 de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115 de 14 de mayo de 1982) que la desarrolla. Es por ello que, durante largo tiempo, los tribunales hayan tenido que detallar los rasgos de la misma a la vista de las ideas que en cada momento prevalecen en la sociedad: «El reconocimiento del derecho a la intimidad personal y familiar tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (artículo 10.1 de la CE), frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o personas particulares, de suerte que atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal, sino también familiar (STC 197/1991, de 17 de octubre de 1991, rec. 492/1989 (LA LEY 1822-TC/1992), frente al conoci-

alcance del derecho a la intimidad en la sociedad actual», en *Revista Derecho del Estado*, n.º 21, diciembre de 2008, pág. 10.

35 MONEREO PÉREZ, J.L. y ORTEGA LOZANO, P.G. «El control empresarial del correo electrónico del trabajador», en *Temas Laborales: Revista andaluza de trabajo y bienestar social*, núm. 150, 2019, págs. 133-159.

36 OROZCO PARDO, G. «Artículo 7. Respeto de la vida privada y familiar», en *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea*, obra colectiva dirigida y coordinada por Cristina Monereo Atienza y José L. Monereo Pérez, Granada, Comares, 2012, págs. 134-156. LÓPEZ DÍAZ, E. «El Derecho al Honor y el Derecho a la Intimidad», Madrid, Dikynson, 1996, págs. 248 y siguientes.

miento de terceros y a la publicidad no querida (sentencias del TC 197/1991, de 17 de octubre de 1991 (mencionada) y 115/2000, de 10 de mayo, rec. 640/1997 (LA LEY 92668/2000), evitando así las intromisiones arbitrarias en la vida privada, censuradas por el artículo 12 de la Declaración Universal de los Derechos Humanos». Por tanto, la intimidad en cuanto concepto de carácter objetivo o material habrá de entenderse referido al área que cada persona guarda para sí o para sus íntimos, apartándola del conocimiento de terceros (STC 170/2013, de 7 de octubre de 2013 (BOE núm. 267 de 7 de noviembre del 2013) y respaldada en la dignidad humana (artículo 10.1 de la CE) como principio guía en todo Estado de Derecho³⁷. La tutela del derecho a la intimidad no se limita exclusivamente a los aspectos más reservados de la vida privada de las personas *stricto sensu*, sino que amplía esa protección a otras manifestaciones que también pueden lesionar la *privacy* como tal³⁸. De modo que sólo cuando medie consentimiento o se haya recabado la preceptiva autorización judicial conforme a criterios de proporcionalidad, se podrán conocer por terceros los aspectos relativos a la privacidad de las personas.

En cuanto derecho fundamental el Tribunal Constitucional nos recuerda en su sentencia 170/2013, de 7 de octubre que «... el derecho a la intimidad no es absoluto —como no lo es ningún derecho fundamental—, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el límite que aquél haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y sea proporcionado» (FJ 5, letra b)). Como consecuencia del recurso de amparo núm. 2907-2011, el Tribunal Constitucional ha entendido que la mera «sospecha» acerca de si un trabajador transmite o no indebidamente información confidencial de su empresa a otra entidad mercantil, constituirá causa suficiente para que el empresario esté legitimado para comprobar tanto el contenido de los mensajes «SMS» del móvil profesional del trabajador, como del disco duro del portátil proporcionado por su empresa (artículo 20.3 ET). A falta de una concreta regulación heterónoma del modo de fiscalización de la correspondencia electrónica privada por la empresa, el Constitucional centra ahora toda su atención en la deficiente ordenación dispuesta por la autonomía colectiva en donde ni se prohíbe, ni se avisa o se dictan las directrices que va a llevar a cabo el empresario para inspeccionar el contenido de las comunicaciones privadas de sus trabajadores. Información que, posteriormente, utilizará como prueba para despedirlos disciplinariamente por transgresión de la buena fe contractual (artículo 54.2 d) ET). Y es que tan sólo se tipifica por el convenio colectivo como falta leve «La utilización de los medios informáticos propiedad de la empresa (correo electrónico, Intranet, Internet...etcétera) para fines distintos de los relacionados con el contenido de la prestación laboral...».

Por lo que, siguiendo la tesis de este tribunal, habrá de prevalecer el interés del empresario (artículo 38 de la CE) por encima del respeto a los derechos fundamentales, lo que determinará finalmente que la efectividad de un derecho inviolable dependa de lo dispuesto por la empresa³⁹. No obstante, olvida el Alto Tribunal que el derecho a la intimidad al penetrar en la relación de trabajo impone límites a la potestad discrecional del empresario actuando, a un mismo tiempo, como garantía del ejercicio de otros derechos fundamentales (en este

37 PÉREZ LUÑO, A. E. «Derechos Humanos, Estado de Derecho y Constitución», Madrid, Tecnos, 1995, págs. 317-318.

38 ROMERO PÉREZ, X.L. «El alcance del derecho a la intimidad en la sociedad actual», en *Revista Derecho del Estado*, número 21, diciembre de 2008, pág. 213.

39 VALDÉS DAL-RÉ, F. «La dimensión laboral de la libertad de expresión», en *Relaciones Laborales*, núm. 7, abril de 2004, pág. 6.

caso del secreto a las comunicaciones y a la dignidad humana). De lo contrario «esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental en su núcleo esencial»⁴⁰. En efecto, la protección del derecho fundamental a la intimidad debe ponderarse con respecto a la defensa de otros derechos, con el fin de garantizar un justo equilibrio entre la tutela de ese derecho (la libertad de empresa) y la salvaguarda de los derechos fundamentales (Véase las conclusiones del Abogado General Sr. Cruz Villalón, presentadas en el asunto C-314/12 UPC *Telekabel Wien GmbH/ Constantin Film Verleih GmbH y Wega Filmproduktionsgesellschaft GmbH*, en su apartado 81 (TJUE). Comunicado de Prensa n.º 149/13, publicada en Luxemburgo a 26 de noviembre del 2013). Así pues «... no debe olvidarse que la Constitución ha querido que la ley, y sólo la ley, pueda fijar los límites a un derecho fundamental, exigiendo además que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido» (FJ 7 de la STC 29/2013, de 11 de febrero de 2013 (BOE núm. 61 de 12 de marzo de 2013).

En esta línea habrá de incluirse también el respeto al secreto de las comunicaciones, toda vez que este derecho actúa como garantía de la intimidad y de la libertad individual. Ciertamente, en una era tecnológicamente avanzada como la presente se ha de amparar no sólo la intimidad de los ciudadanos, sino por ende la tutela de aquellas otras injerencias que derivan de la misma y, en particular, de los derechos que recogen los apartados 2, 3 y 4 del texto constitucional.

3.2. La protección de los derechos fundamentales en relación con las nuevas tecnologías

El derecho a la intimidad, al hilo de las nuevas tecnologías, se relaciona con derechos fundamentales tales como: la dignidad, la propia imagen y el secreto a las comunicaciones. A este respecto, se ha planteado en la doctrina de los tribunales todo un debate que aún no cesa. Especialmente relevante es la relación del derecho a la intimidad con el secreto a las comunicaciones y en relación al uso que del ordenador o de los nuevos dispositivos electrónicos hagan los trabajadores.

Podría afirmarse que, desde la Constitución Española de 1869, el derecho al secreto de las comunicaciones se ha visto varias veces modificado y ampliado en su ámbito de cobertura, evolucionando conforme se transforma la sociedad y abarcando situaciones que por aquel entonces eran completamente inimaginables para el legislador (Previamente a esta normativa, ya se había configurado el derecho a la libertad y al secreto a la correspondencia con la Revolución Francesa. Así, en la Asamblea Nacional en 1790 se proclamó este principio como sigue: «*Le secret des lettres est inviolable*»). Actualmente y tras un largo proceso de desarrollo, se ha regulado este derecho en el artículo 18.3 de la Norma Madre que establece que: «Se garantizará el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial». Pese a su ubicación constitucional, no se han concretado en esta norma los supuestos que cubre y ello porque el constituyente de 1978 fue consciente de que con el paso del tiempo podía llegar a experimentarse cambios sociales y tecnológicos que alterasen profundamente las reglas inicialmente previstas. Así pues, insertó

40 ICHINO, P. «Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro», Milano, Giuffrè, 1979, pág.52.

un sistema *numerus apertus* o de listas abierta sujeto a los posibles cambios de la realidad social presente (en esta tónica, el vigente artículo 15 de la Constitución Italiana dispone: «Será inviolable la libertad y el secreto de las comunicaciones cualquiera que sea la forma de intromisión en las mismas. Únicamente se podrán limitar el ejercicio de estos derechos mediante resolución motivada de la autoridad judicial y siempre que quede garantizada que esta injerencia se ajusta a los supuestos que son enumerados en la ley»). En vista de que la ley no puede implicar una rigidez excesiva, el Derecho debe saber adaptarse y adecuar su ordenación a los cambios culturales contemporáneos.

A este respecto, ha señalado el Tribunal Constitucional en su sentencia 70/2002 de 3 de abril que: «Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE». Ciertamente, la protección del derecho al secreto a las comunicaciones no se limita en exclusiva a las postales, telegráficas o correspondencia privada (cartas), sino que se extiende a todas las comunicaciones (electrónicas y no electrónicas) puestas a disposición de las nuevas TIC, ya sea a través de cable, de forma inalámbrica o mediante conmutador analógico o digital, independientemente de si se trata de expresiones del lenguaje, imágenes, sonidos u otros datos (TC Federal Alemán en su sentencia de 2/03/2006). El marco de protección de este medio de comunicación no encuentra limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse. Por lo que podrá encuadrarse dentro de este marco constitucional también las comunicaciones mantenidas por telefonía móvil, así como por mensajería (mns) y las telemáticas. En esta línea, se ha pronunciado las Sentencias del TEDH de 10 de marzo del 2009 (caso Bykov vs Rusia, asunto 4378/02) respecto de las comunicaciones radiofónicas, y de 16 de octubre de 2007 (caso Wieser y Bicos Beiligungen GMBH vs. Austria, asunto 74336/01) y 22 de mayo del 2008 (caso Ilija Stefanov vs. Bulgaria, asunto 65755/01) para las telemáticas.

La irrupción de los denominados derechos de tercera y cuarta generación, entre los que se incluye internet, ha dificultado enormemente su integración en los esquemas tradiciones que marca el legislador de 1978. Ello por no mencionar su imperfecta ordenación a la hora de tratar de solucionar los conflictos que se generan en la práctica⁴¹. De ahí que los tribunales se esfuercen por colmar las lagunas existentes arrojando interpretaciones que, en algunos casos, resultan análogas a las aplicadas para otras situaciones, pero que en verdad son distintas a las que hoy día se desarrollan por las empresas a través del mundo cibernético. Atentando así de manera peligrosa contra el núcleo mismo del derecho al secreto de las comunicaciones⁴².

Efectivamente, el cambio de hábitos en la comunicación intrapersonal ha roto la clásica relación de alteridad (emisor-receptor) que anteriormente constituía la esencia misma de la transmisión de información. La razón es que internet ha creado y fomentado otros métodos

41 MONEREO PÉREZ, J.L. «La protección de los derechos fundamentales. El modelo europeo», Albalade, Bomarzo, 2009, págs. 121-122.

42 SEGOVIANO ASTABURUAGA, M.L. «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», en *Revista Jurídica de Castilla y León*, núm. 2, febrero de 2004, pág. 157.

de comunicación en donde el receptor de la información puede convertirse en proveedor de ésta por sí mismo o a través del reenvío de los datos a través de un tercero. De este modo las TIC permiten ahora el desarrollo de nuevos sistemas de expresión y relación entre individuos que, en algunos casos, podrán ser objeto de control por el empresario a fin de inspeccionar los movimientos que realizan sus trabajadores⁴³.

Al igual que ocurre en territorio nacional, la UE ha tenido también en cuenta esa «evolución técnica» y la afección que puede suponer a la intimidad. De ahí que todas las políticas que desde el colectivo comunitario se han desarrollado vayan enfocadas a la protección de la *privacy* en el ámbito de los sistemas de información. En este sentido se habrán de tener en cuenta los derechos que reconoce el artículo 12 de la Declaración de Derechos Humanos de 1948; el artículo 17 del Pacto de Derechos Civiles y Políticos; el artículo 8.1 del CEDH y el artículo 7 de la CDFUE. Todos ellos son derechos que conllevan un conjunto de facultades que, en función del momento histórico, determinarán las exigencias de libertad, igualdad y dignidad reconocidas por el ordenamiento jurídico nacional e internacional a todas las personas.

3.3. Biométrica, «Big Data» y datos personales en la Ley de Protección de Datos: la judicialización de los conflictos

El Reglamento General de Protección de Datos establece que el manejo y almacenamiento de datos biométricos y personales de las personas se eleva a la categoría de «especialmente protegidos», siempre que se usen para «identificar de manera unívoca a una persona física», por lo que a fin de no vulnerar los derechos fundamentales implicados (a saber: derecho a la intimidad, al honor, a la dignidad, a la propia imagen, etcétera), se establecen una serie de garantías. Por lo tanto, todo lo relativo a la identidad física de una persona se considera como «datos sensibles».

En este sentido, el RGPD identifica a los datos biométricos como «sensibles» según la legislación de la Unión Europea. De acuerdo con esta idea, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD)⁴⁴ se refiere al tema de los datos biométricos de manera residual y a través de las disposiciones adicionales.

En línea con el RGPD, el artículo 9 de la LOPD identifica los datos biométricos como una «categoría especial de datos» al señalar que «... el consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico».

Ahora bien, la disposición final undécima matiza que «si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se

43 SÁNCHEZ TORRES, E. «El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías», en *Relaciones Laborales y Nuevas Tecnologías*, obra colectiva dirigida por S. Del Rey Guanter y coordinada por M. Luque Parra, Madrid, La Ley, 2005, págs. 108-109.

44 BOE núm. 294 de 6 de diciembre de 2018.

podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley».

En esta misma línea, se pronuncia el Tribunal de Justicia de la Unión Europea (Sala cuarta) en su sentencia de 26 de enero de 2023 (Asunto C-205/21: *Ministerstvo na vatreshnite raboti*). En particular, el Tribunal de Justicia de la Unión Europea (en adelante TJUE) recalca que sólo podrá autorizarse los datos biométricos cuando son con fines de lucha contra la delincuencia y el tratamiento del orden público y siempre que, ese derecho, contenga una base jurídica suficientemente clara y precisa que lo autorice. Por otra parte, recalca este tribunal que, aunque la legislación nacional se remita al RGPD ello no desvirtúa la regulación que, a nivel comunitario, se establece por la Directiva marco. A *sensu contrario*, se autoriza la recogida de datos biométricos cuando haya una autorización judicial (aunque la persona sea inocente), aunque se condiciona todo a que el derecho nacional garantice, posteriormente, el control jurisdiccional efectivo de esa investigación. El TJUE tiene que claro que, si hay otros cauces «menos gravosos» para obtener información de una persona, la normativa nacional habrá de poner en funcionamiento esas vías para preservar la intimidad de la persona.

En resumen y siguiendo las palabras del TJUE:

«... el Tribunal de Justicia subraya que la Directiva 2016/680 pretende garantizar, entre otras cosas, una mayor protección con respecto a los tratamientos de datos sensibles, entre los que figuran los datos biométricos y genéticos, puesto que pueden generar riesgos importantes para las libertades y los derechos fundamentales. El requisito que en ella se menciona que tales tratamientos «solo» se permitirán «cuando sea estrictamente necesario» debe interpretarse en el sentido de que define unas condiciones reforzadas de licitud del tratamiento de datos sensibles. Además, se ha de determinar también el alcance de este requisito a la luz de principios relativos al tratamiento de los datos tales como la limitación de los fines y la minimización de los datos».

Siguiendo este orden de ideas: ¿Cuándo y cómo podrá una empresa tratar los datos biométricos de sus trabajadores? Para ello debemos remitirnos al artículo 9 del RGPD, en donde se enumeran varios supuestos:

- a) Por consentimiento explícito del interesado, esto es, cuando el sujeto manifiesta de manera clara e inequívoca su aprobación a través de una acción afirmativa.
- b) Cuando se deba proteger el interés vital del interesado cuando éste se encuentre incapacitado para tomar decisiones.
- c) Cuando sea necesario para el cumplimiento de obligaciones establecidas o para llevar a cabo los derechos de la protección de datos.
- d) En el supuesto de que los datos sean públicos y haya sido el interesado quien los haya publicado.
- e) Por interés público esencial siempre que sea proporcional al objetivo perseguido.
- f) Finalmente, cuando esos datos sean empleados para fines de medicina preventiva, cuestiones sociales o para evaluar capacidades del trabajador.

Aparte de los límites empresariales al control empresarial que prevé el artículo 20 del Estatuto de los Trabajadores y las garantías para los trabajadores, las empresas deberán cumplir con una serie de obligaciones de protección de datos a fin de no vulnerar los derechos fundamentales implicados.

En primer lugar, cabe hablar del «deber de información», esto es, cuándo y cómo se van a solicitar los datos biométricos a los interesados. Aparte, habrá de informarse sobre los encargados del tratamiento o de sus representantes, la finalidad del tratamiento, el plazo de conservación de datos, la cesión de datos a terceros o las vías para ejercer sus derechos ARSULIPO (se corresponde con el «acceso», la «supresión», la «limitación», la «portabilidad» y la «oposición»).

En segundo lugar, se debe recabar el «consentimiento de los afectado». De igual modo, quedará la empresa obligada a cumplir con el «deber de seguridad» (en tercer lugar). Y es que los responsables del tratamiento han de aplicar de manera proactiva todas las medidas necesarias para garantizar la seguridad e integridad de la información. Y, todo ello, con el objetivo de evitar la pérdida o el robo de datos o los accesos por parte de terceros no autorizados. También han de informar a la Agencia Española de Protección de Datos si se produce una brecha de seguridad en un plazo de 72 horas.

Siguiendo con la obligación de respetar la intimidad de los trabajadores afectados, la empresa deberá respetar —en cuarto lugar— la «confidencialidad» de los datos recabados, no pudiendo revelarla a terceros. Eso incluye la obligación de firmar un acuerdo de confidencialidad con los encargados del tratamiento o con los empleados que tengan acceso a los datos biométricos.

De cara a prevenir posibles efectos adversos, en quinto y sexto lugar, las empresas habrán de «evaluar el impacto» de las medidas adoptadas, al tiempo que cumplen con los principios de «necesidad, idoneidad y proporcionalidad del tratamiento». Los datos biométricos deben ser recogidos para unos fines determinados y no podrá la empresa extralimitarse de sus competencias. Asimismo, si para obtener un fin existen medios menos gravosos e intrusivos, deberá ésta aplicar éstos en lugar de los datos biométricos. En caso de no hacerlo, se invertirá aquí la carga de la prueba, quedando la empresa obligada a demostrar la «idoneidad y necesidad» de la medida adoptada. Y no pueden realizarse tratamientos distintos a los que se recojan en el consentimiento prestado por el interesado. Por su parte, el principio de necesidad implica que los datos biométricos que se vayan a recabar deben ser los adecuados y nunca excesivos para los fines que se vayan a tratar. El principio de idoneidad y proporcionalidad hace referencia a los riesgos que se entrañan para la protección de los derechos y libertades fundamentales de las personas. Y para cuando los fines no pueden alcanzarse de otra forma menos agresiva.

En último lugar, cabe hablar del «registro de las actividades objeto de tratamiento», pues todos los datos recabados habrán de quedar bajo el control de una determinada entidad. A este respecto, la base de datos biométricos habrá de contener como mínimo la siguiente información: a) nombre y datos de contacto (de los responsables, los encargados, los representantes y el delegado de protección de datos), b) fines del tratamiento, c) la descripción de las categorías de los interesados y de los datos personales y d) los plazos previstos para la supresión o la eliminación de las diferentes categorías de datos.

El tratamiento de los datos que puedan hacer las empresas, a efectos de control, identificación y constatación de la presencia de los mismos en el puesto de trabajo se considera una medida de seguridad para la empresa. La empresa está facultada para adoptar estas medidas, siempre que informe sobre el tratamiento que de los datos biométricos va a realizar. Ahora bien, a cuestión más litigiosa sobrevuela en torno a la figura del «consentimiento». ¿Resulta necesario recabar el consentimiento expreso en todos los casos? Cabe traer a colación aquí la sentencia del Tribunal de Justicia de la Unión Europea de 30 de marzo de 2023, en el asunto C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer).

En la mentada sentencia se debate sobre el tema del consentimiento de los profesores de enseñanzas escolares a la hora de participar en sistema de videoconferencia. Los hechos se remontan al año 2020, en concreto, cuando se declaró la pandemia del COVID-19 a nivel mundial. Mediante dos actos adoptados en 2020, el Ministro de Educación y Cultura del Estado Federado de Hesse (Alemania) estableció el marco jurídico y organizativo de la enseñanza escolar durante el período de pandemia de COVID-19, estableciendo, en particular, la posibilidad de que los alumnos que no pudieran estar presentes en clase asistieran en directo a las clases por videoconferencia. Con el fin de preservar los derechos de los alumnos en materia de protección de datos personales, se dispuso que la conexión al servicio de videoconferencia solo se autorizaría con el consentimiento de los propios alumnos o, en caso de minoría de edad de estos, de sus padres. En cambio, no se prescribió el consentimiento de los docentes implicados a su participación en dicho servicio.

Censurando que la difusión en directo de las clases por videoconferencia, tal como estaba regulada por la normativa nacional, no estuviera supeditada al requisito del consentimiento de los docentes implicados, el Comité Principal del Personal Docente del Ministerio de Educación y Cultura del Estado Federado de Hesse interpuso un recurso contra el ministro competente en la materia. Este alegó que el tratamiento de datos personales que constituye la difusión en directo de las clases por videoconferencia estaba cubierto por la normativa nacional, de modo que podía realizarse sin solicitar el consentimiento de los docentes implicados.

El órgano jurisdiccional de lo contencioso-administrativo que conoció del asunto indicó que, de conformidad con la voluntad del legislador del estado federado de Hesse, la normativa nacional sobre cuya base se realiza el tratamiento de los datos personales de los docentes pertenece a la categoría de las «normas más específicas» que los Estados miembros pueden establecer, de conformidad con el artículo 88, apartado 1, del Reglamento general de protección de datos⁴⁵, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral⁴⁶. No obstante, dicho órgano jurisdiccional alberga dudas en cuanto a la compatibilidad de dicha normativa con las exigencias impuestas por el artículo 88, apartado 2, del RGPD, en donde

45 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

46 De acuerdo con el artículo 88 del RGPD, los Estados miembros tienen la facultad de establecer, por ley o por convenio colectivo, «normas más específicas» para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, a efectos, en particular, de ejecución del contrato laboral, gestión, planificación y organización del trabajo.

se recoge el derecho a la «dignidad» humana de los interesados⁴⁷. Por lo tanto, presentó una petición de decisión prejudicial ante el Tribunal de Justicia de la Unión Europea.

Visto el caso anunciado, el TJUE entiende que el tratamiento de datos personales de los docentes (a través de la difusión en directo de su imagen por videoconferencia) constituye una materia incluida dentro del Reglamento General de Protección de Datos Personales, por lo que, cabe aquí hacer valer las garantías que prevé el artículo 88 del Reglamento. En este sentido, una normativa nacional no podrá nunca imponerse a lo dispuesto al Reglamento, ni tampoco podrá constituir una «norma más específica» a los efectos del apartado 1, del artículo 88 del RGPD. Por lo que, si no se cumplen con las garantías que prevé el respeto a la «dignidad» y a la protección de los derechos fundamentales, podrá el interesado o los interesados invocarse la aplicación del RGPD.

Adicionalmente, recalca este tribunal la necesidad de que el juez nacional controle la adecuación o no de una normativa nacional respecto a los límites establecidos en el RGPD. No obstante, el Tribunal de Justicia de la UE señala que esas disposiciones nacionales, que supeditan el tratamiento de los datos personales de los empleados a la condición de que dicho tratamiento sea necesario para determinados fines relacionados con la ejecución de una relación laboral, parecen reiterar la condición para la licitud general ya establecida en el Reglamento General de Protección de Datos, sin añadir una norma más específica en el sentido del artículo 88, apartado 1, de dicho Reglamento. En el supuesto de que el órgano jurisdiccional remitente llegara a la conclusión de que las disposiciones nacionales no respetan las condiciones y los límites establecidos por el artículo 88 del RGPD, le correspondería, en principio, dejarlas inaplicadas. En efecto, en virtud del principio de la primacía del Derecho de la Unión, a falta de normas más específicas que respeten las condiciones y los límites establecidos en el artículo 88 del RGPD, el tratamiento de datos personales en el ámbito laboral, tanto en el sector privado como en el público, se rige directamente por las disposiciones de dicho Reglamento.

IV. Prevención de riesgos laborales: nuevos riesgos. Teletrabajo y derecho a la desconexión digital

El empleo de las nuevas tecnologías ofrece pros y contras que se hacen visibles en el ámbito de las relaciones laborales. Por una parte, este fenómeno ofrece ventajas de eficiencia en la utilización de los recursos, mejoras competitivas, mayor oferta de productos, mayor interacción entre el trabajador y el cliente, reforzamiento de la formación y empleabilidad de las personas trabajadoras... etcétera. Sin embargo, por otro lado, la máscara de las nuevas tecnologías y del trabajo a distancia también presenta múltiples inconvenientes, entre los que se encuentra el alargamiento de la jornada laboral y del lugar de trabajo, más allá del ámbito

47 En particular, los Estados habrán de incluir reglas que prevean medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales y a los sistemas de supervisión en el lugar de trabajo.

de la empresa, lo que igualmente puede determinar una falta de conciliación de la vida laboral y familiar e incluso una sobrecarga del trabajador expuesto, con motivo de esa flexibilización de los conceptos «lugar» y «tiempo de trabajo» (Exposición de Motivos de la Ley 10/2021, de 9 de julio, de trabajo a distancia –BOE núm. 164 de 10 de julio de 2021–). Aparte, cabe considerar la dependencia tecnología que puede generarle al trabajador y la sobrecarga de información, tanto a la hora del acceso a la misma como al de su recepción. Todo ello determina el surgimiento de conceptos como el de «hot desker» (trabajadores sin ubicación física fija en el centro de trabajo), espacios de «coworking» o «techub» (espacios donde una red internacional de emprendedores pueda trabajar, relacionarse, colaborar y aprender).

Efectivamente, el uso de las nuevas tecnologías permite desarrollar la actividad laboral fuera del centro de trabajo y del propio horario laboral. Con independencia del trabajo a distancia regulado en el artículo 13 del ET, subsiste una cierta tolerancia social ante el uso moderado en el trabajo de las nuevas tecnologías para fines personales, con independencia del título de propiedad de las mismas, en sentido inverso, también existe esa condescendencia a la hora de utilizar –igualmente de manera moderada– para fines laborales, pero fuera del lugar de trabajo y de la jornada laboral, esas nuevas tecnologías, sean o no propiedad del empleador, extendiéndose la jornada laboral más allá del horario prefijado. Los límites en esta materia son algo difusos, sobre todo cuando una situación que ha de ser excepcional se termina convirtiendo en la tónica habitual, lo que en definitiva no deja de ser una prolongación de la jornada laboral, un tiempo extraordinario de trabajo generalmente no compensado económicamente y no cotizado, que además repercute en la salud del trabajador, que ha de descansar entre jornadas (esto es lo que llamamos desconexión digital).

Al hilo de este tema, cabe tener presente el tema del teletrabajo, pues a raíz de la pandemia protagonizada por el coronavirus se han impuesto como una opción preferente (RD 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 y se publica el Decreto ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19). Al tiempo que se eliminan las posibilidades de contagio por COVID-19, aparecen otros nuevos riesgos que pueden afectar a la salud del trabajador y, por ende, a la misma condición de «trabajo decente». Esencialmente este lance se hace mayor en mujeres que en hombres, pues son todavía mayoritariamente ellas las que se encargan del cuidado y el mantenimiento del hogar familiar⁴⁸. Aunque en un principio pudiera parecer que ello facilita la conciliación de la vida familiar y laboral (así como la inserción de colectivos marginados en el mundo laboral, a saber: los discapacitados), lo cierto es que ello puede provocar también sobrecarga laboral y agotamiento. Por supuesto, debe tenerse en cuenta también los factores antes mencionados de volumen de tareas, nivel de responsabilidad, la libertad individual para regular el ritmo de trabajo... etcétera. Sin embargo, ya se encuentran trabajadores que han desarrollado problemas de falta de distinción entre el trabajo y la vida familiar y social. Muy relacionado con este dato se encuentra el concepto de interrupción y pausa en el trabajo, que tiene mayor probabilidad de producirse en los teletrabajadores. Entiendo, por lo tanto, que una combinación satisfactoria entre el trabajo y la vida socio-familiar exige separar claramente el lugar de trabajo y una serie de normas comunes acordadas en relación con la concentración no interrumpida del trabajo. Ciertamente, la empresa ostenta ahí un poder esencial para la prevención, detección de estos riesgos y la garantía de un trabajo en condiciones de calidad.

48 LÓPEZ INSUA, B.M. *El principio de igualdad de género en el Derecho Social del Trabajo*, Murcia, Laborum, 2017.

Para ello, la empresa debe realizar un estudio de viabilidad teniendo en cuenta cuestiones personales, de espacio y relacionadas con el trabajo (esto es, trabajos basados en proyectos, interrupciones frecuentes...etcétera). Y todo ello, conforme a unos criterios de selección y procedimientos claramente determinados⁴⁹.

Relacionada con esta idea, la «Estrategia Española de Seguridad y Salud en el Trabajo 2015-2020» hace referencia a los riesgos derivados de las nuevas tecnologías, incluyéndolos bajo la denominación de «riesgos emergentes», riesgos que en ese momento se consideraban prioritarios, recalcando la necesidad de analizar sus causas e impactos en la seguridad y salud de los trabajadores. Contempla que la irrupción de las TIC's producirá lugares de trabajo más flexibles, oficinas virtuales y teletrabajo. Por ello acuden a la necesidad de establecer programas de vigilancia de los trabajadores expuestos a ellos.

Recuérdese, además, que el artículo 14 de la Ley 31/1995 de Prevención de Riesgos Laborales impone al empresario una serie de obligaciones para garantizar la seguridad y la salud en el trabajo del trabajador y, correlativamente, reconoce al trabajador el derecho a una protección eficaz en esta materia. En particular, el punto 2 de este artículo señala que: «En cumplimiento del deber de protección, el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo. A estos efectos, en el marco de sus responsabilidades, el empresario realizará la prevención de los riesgos laborales mediante la integración de la actividad preventiva en la empresa y la adopción de cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores, con las especialidades que se recogen en los artículos siguientes en materia de plan de prevención de riesgos laborales, evaluación de riesgos, información, consulta y participación y formación de los trabajadores, actuación en casos de emergencia y de riesgo grave e inminente, vigilancia de la salud, y mediante la constitución de una organización y de los medios necesarios en los términos establecidos en el capítulo IV de esta ley». Asimismo, el Instituto Nacional de Seguridad y Salud en el Trabajo define los riesgos psicosociales como: «... aquellas condiciones presentes en una situación laboral directamente relacionadas con la organización del trabajo y su entorno social, con el contenido de trabajo y la realización de la tarea y que se presentan con capacidad para afectar el desarrollo del trabajo y la salud (física, psíquica o social) del trabajador». Y continúa exponiendo que: «... unas condiciones psicosociales adversas están en el origen tanto de determinadas conductas y actitudes inadecuadas en el desarrollo del trabajo como de determinadas consecuencias perjudiciales para la salud y para el bienestar del trabajador».

Aparte de los problemas psicosociales que pueden derivar del trabajo, aparecen además algunas consecuencias físicas como las malas posturas y los problemas musculares, en el caso de que los lugares de trabajo donde éste desarrolle sus funciones no cumplan con la normativa sobre seguridad y ergonomía. Principalmente, destacan los dolores de cuello, muñeca, dedos y espalda. Además de ellos, pueden aparecer problemas oftalmológicos de mayor o menor acentuación, así como trastornos en el sueño. Para paliar los diferentes trastornos, los servicios de prevención deben proponer medidas técnicas, además de formación y vigilancia de la salud, de modo que el trabajador pueda gestionar los tiempos de manera adecuada.

49 LÓPEZ INSUA, B.M. «Trabajo decente y prestaciones ante situaciones de necesidad (I): Incapacidad para trabajar», en *El trabajo decente*, obra colectiva dirigida por José L. Monereo Pérez, Juan Gorelli Hernández y Ángel L. De Val Tena y coordinada por Belén del M. López Insua, Granada, Comares. Colección Trabajo y Seguridad Social núm. 111, 2018.

Los principales problemas que aparecen relacionados con el uso de las nuevas tecnologías están relacionados, principalmente, con la distribución temporal del trabajo y la interferencia del mismo con el tiempo libre o de ocio. Además, cabe considerar otros problemas relacionados con altas exigencias y la inmediatez de respuesta, los plazos ajustados, la fatiga mental y el cansancio debido a la disponibilidad permanente. Otros condicionantes como las tareas rutinarias, trabajar con demasiada información o trabajar contrarreloj, cobran una importancia especial cuando se usan las nuevas tecnologías, lo que conllevaría la necesidad de controlar estas condiciones de trabajo, por ejemplo, a través de la regulación en el convenio colectivo o de protocolos negociados. Lo que determinaría una mayor implicación de los agentes negociadores.

Sobre estas cuestiones, la normativa de prevención de riesgos laborales resalta la importancia de realizar una evaluación de los riesgos psicosociales en el trabajo, seguida de una planificación de la actividad preventiva (artículos 16 de la Ley 31/1995 de Prevención de Riesgos Laborales) y aplicándose, en caso necesario, las pertinentes medidas preventivas. Sobre este punto la Ley 10/2021, de 9 de julio, de trabajo a distancia específica, en su artículo 16.1, que la «evaluación y planificación de la actividad preventiva en el trabajo a distancia deberán tener en cuenta los riesgos característicos de esta modalidad de trabajo, poniendo especial atención en los factores psicosociales, ergonómicos y organizativos y de accesibilidad del entorno laboral efectivo. En particular, deberá tenerse en cuenta la distribución de la jornada, los tiempos de disponibilidad y la garantía de los descansos y desconexiones durante la jornada. La evaluación de riesgos únicamente debe alcanzar a la zona habilitada para la prestación de servicios, no extendiéndose al resto de zonas de la vivienda o del lugar elegido para el desarrollo del trabajo a distancia...». De modo que se preserve la salud del trabajador, al tiempo que se reserva la intimidad del trabajador. Finalmente, los trabajadores habrán de recibir la formación adecuada y específica de conformidad a las exigencias de su puesto de trabajo.