

Nuevas fórmulas de prestación de servicios en la era digital

Dirección:

Federico A. Castillo Blanco
Juan Francisco Pérez Gálvez

Coordinación:

Susana E. Castillo Ramos-Bossini



**NUEVAS FÓRMULAS
DE PRESTACIÓN DE SERVICIOS
EN LA ERA DIGITAL**

NUEVAS FÓRMULAS DE PRESTACIÓN DE SERVICIOS EN LA ERA DIGITAL

DIRECTORES:

FEDERICO A. CASTILLO BLANCO

JUAN FRANCISCO PÉREZ GALVEZ

COORDINADORA:

SUSANA E. CASTILLO RAMOS-BOSSINI

Dykinson, S.L.

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web www.conlicencia.com o por teléfono en el 917021970/932720407.

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial.
Para mayor información, véase www.dykinson.com/quienes_somos

© Copyright by
Los autores

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69
e-mail: info@dykinson.com
<http://www.dykinson.es>
<http://www.dykinson.com>

ISBN: 978-84-1170-731-2
Depósito Legal: M-35469-2023

ISBN electrónico: 978-84-1070-000-0

Preimpresión por:
Besing Servicios Gráficos S.L.
e-mail: besinasa@gmail.com

Proyecto TED2021-131550B-I00 financiado por:



MINISTERIO
DE CIENCIA
E INNOVACIÓN



Financiado por
la Unión Europea
NextGenerationEU



CONSEJO
SUPERIOR DE
INVESTIGACIONES
CIENTÍFICAS



UNIVERSIDAD
DE GRANADA



SOCIEDAD DIGITAL
SEGURIDAD Y PROTECCIÓN DE DERECHOS
Unidad de Excelencia de Investigación

Índice

La influencia de la transformación digital en el ámbito tributario..... 15

MARÍA-JOSÉ FERNÁNDEZ-PAVÉS

I.	CONTEXTO ACTUAL FAVORABLE	15
II.	PUNTO INICIAL: LA LEY GENERAL TRIBUTARIA.....	21
	II.1. Referencia expresa a la digitalización en el ámbito tributario	21
	II.2. Marco normativo general.....	22
	II.3. Ámbitos donde pueden utilizarse medios digitales	24
	II.4. Actuaciones necesariamente digitales	27
	II.5. Limitaciones a su imposición al ciudadano por la Administración tributaria	30
III.	ESTUDIO DE ALGUNAS ACTUACIONES TRIBUTARIAS DIGITALIZADAS.....	35
	III.1. Información y asistencia digital a los obligados tributarios.....	36
	III.2. Digitalización de los procedimientos tributarios	40
	III.3. Resoluciones administrativas automatizadas.....	44
	III.4. Breve referencia a las notificaciones tributarias electrónicas	47
IV.	PERSPECTIVAS A CONSIDERAR PARA EL FUTURO.....	51
V.	BIBLIOGRAFÍA.....	53

El servicio educativo: aprendizaje personalizado y educación automatizada 55

LEONOR MORAL SORIANO

I.	CONCEPTO (NORMATIVO) DE INTELIGENCIA ARTIFICIAL.....	55
II.	DERECHO A LA EDUCACIÓN	57
III.	LAS TECNOLOGÍAS EDUCATIVAS (EDTEC)	60
	III.1. Los inicios de la EdTech.....	61
	III.2. La minería de datos de la EdTech	63
	III.3. La educación personalizada de las EdTech.....	69
IV.	DEL APRENDIZAJE PERSONALIZADO AL APRENDIZAJE AUTOMÁTIZADO	71
V.	EL APRENDIZAJE AUTOMATIZADO NO ES EL BÁLSAMO DE FIERABRÁS.....	76
	V.1. Alcance de la tecnología	77
	V.2. Qué educación para qué contexto.....	79
VI.	BIBLIOGRAFÍA.....	85

La transformación digital en el ámbito sanitario 89

JUAN FRANCISCO PÉREZ GÁLVEZ

I.	EL PUNTO DE PARTIDA: LA LLEGADA DE LA ADMINISTRACIÓN ELECTRÓNICA, EVOLUCIÓN DIGITAL E INCIDENCIA EN EL SECTOR SANITARIO.....	90
I.1.	Administración electrónica en el contexto de un mundo digital	90
I.2.	Incidencia del ámbito electrónico en la salud y en la asistencia sanitaria	95
II.	¿DÓNDE ESTAMOS? EL CONTEXTO DE UNA SOCIEDAD DEMOGRÁFICAMENTE ENVEJECIDA Y SOCIALMENTE NECESITADA DE LOS ADELANTOS TECNOLÓGICOS.	104
II.1.	Contexto demográfico y social	104
II.2.	Las nuevas tecnologías son una herramienta básica que permite hacer frente a la realidad demográfica y al incremento del gasto que supone el envejecimiento de la población	113
II.3.	Alfabetización y capacitación electrónica y digital	114
II.4.	La situación de la salud electrónica en la UE y la necesaria transición a la salud digital	122
II.5.	Salud electrónica y nuevas aplicaciones científicas	143
III.	LA DIGITALIZACIÓN DE LA SALUD: UN MODO DISTINTO DE CONCEBIR Y REALIZAR LAS ACTIVIDADES	146
IV.	COROLARIO.....	154
IV.1.	Actuaciones que debemos emprender	154
IV.2.	El proceso de cambio	162
V.	BIBLIOGRAFÍA.....	169

Digitalización e inteligencia artificial en la prestación de servicios públicos asistenciales 173

PAULA M^a TOMÉ DOMÍNGUEZ

I.	INTRODUCCIÓN.....	173
II.	DESAFÍOS ÉTICOS Y NORMATIVOS DE LA INCORPORACIÓN DE LA IA EN LA DETERMINACIÓN DE LA PRESTACIÓN DE SERVICIOS PÚBLICOS ASISTENCIALES	175
III.	INTELIGENCIA ARTIFICIAL: MARCO NORMATIVO ACTUAL.....	180
III.1.	Del escueto marco normativo nacional	180
III.2.	Propuesta de Reglamento UE: enfoque transversal de la gestión de riesgos asociados a la IA y su implicación en el Sector Público	183
III.3.	La determinación del acceso a prestaciones públicas asistenciales: sistemas de alto riesgo	189
IV.	CONCLUSIONES	193
V.	BIBLIOGRAFÍA.....	194

La digitalización del planeamiento urbanístico y de su información..... 197

JESÚS BOBO RUIZ

I.	PLANTEAMIENTO	197
II.	INTRODUCCIÓN. CONVERGENCIA JURÍDICA, URBANÍSTICA E INFORMÁTICA	198
III.	CONTEXTO TÉCNICO DE LA DIGITALIZACIÓN CON ALGUNAS NOTAS JURÍDICAS.....	201
	III.1. Digitalización del documento: métodos ráster	201
	III.2. Digitalización, modelos vectoriales y georreferenciación.....	204
	III.3. Sistemas de Información Geográfica.....	205
	III.4. Integración de la Modelización digital de la edificación (BIM) con los Sistemas de Información Geográfica. La integración BIM-GIS	207
	III.5. Las infraestructuras de datos espaciales.....	211
	III.6. Inteligencia Artificial y Planeamiento urbanístico.....	212
IV.	LA DIRECTIVA INSPIRE COMO PROMOTORA DE LA DIGITALIZACIÓN DEL PLANEAMIENTO URBANÍSTICO Y DE SU INFORMACIÓN.....	214
	IV.1. Aproximación sistemática	214
	IV.2. Geoportal Inspire	219
	IV.3. Datos y conjunto de datos espaciales. el anexo III de la Directiva Inspire	221
	IV.4. Transposición	222
V.	EL SISTEMA DE INFORMACIÓN URBANA (SIU)	223
VI.	PUBLICIDAD EN LA TRAMITACIÓN Y APROBACIÓN DEL PLANEAMIENTO ...	233
	VI.1. Publicación del instrumento.....	234
	VI.2. Consultas públicas.....	237
	VI.3. Publicación de diferentes trámites previos a su aprobación.....	239
VII.	REGISTROS AUTONÓMICOS DE PLANEAMIENTO	240
	VII.1. Marco competencial	240
	VII.2. Los registros autonómicos de planeamiento. el modelo valenciano	243
VIII.	TENDENCIAS Y CONCLUSIONES.....	245
IX.	BIBLIOGRAFÍA.....	246

Los cambios en la prestación de los servicios públicos como consecuencia de la transformación digital: el caso del transporte urbano de viajeros 249

FEDERICO A. CASTILLO BLANCO

I.	INTRODUCCIÓN: LA REVOLUCIÓN DE LA TECNOLOGÍA INFORMÁTICA EN EL SECTOR DEL TRANSPORTE URBANO DE VIAJEROS.....	249
II.	LOS PRIMEROS COMPASES DEL CONFLICTO JUDICIAL EN EL TRANSPORTE TERRESTRE DE VIAJEROS	256

III.	LA RESPUESTA DEL LEGISLADOR A LA PROBLEMÁTICA SUSCITADA Y LA REACCIÓN JURISPRUDENCIAL.....	259
	III.1. El Decreto-ley Ábalos	259
	III.2. La controversia judicial a nivel nacional.	261
	III.3. El pronunciamiento del Tribunal de Justicia de la Unión Europea	265
IV.	VUELTA A LAS ANDADAS: LA ÚLTIMA RESPUESTA DEL LEGISLADOR A TRAVÉS DEL DECRETO-LEY ESCOBA DE 2023.....	268
V.	LA TECNOLOGÍA COMO FUENTE DE TRANSFORMACIÓN DE LA COMPETENCIA: LA COMPETENCIA MUNICIPAL EN EL TRANSPORTE PÚBLICO DE VIAJEROS EN EL ÁMBITO URBANO.....	271
VI.	CONCLUSIONES: NUEVOS TIEMPOS, NUEVAS SOLUCIONES	274
VII.	REFERENCIAS BIBLIOGRÁFICAS	277

La transformación digital en las ciudades: regulación, protección de derechos y brecha digital en las ciudades inteligentes 279

FRANCISCO JAVIER DURÁN RUIZ

I.	INTRODUCCIÓN. CIUDADES INTELIGENTES: TECNOLOGÍA AL SERVICIO DE LOS CIUDADANOS Y SOSTENIBILIDAD	279
II.	REGULACIÓN Y RIESGOS DE LAS CIUDADES INTELIGENTES	285
	II.1. Los datos personales y su protección en la era de la Inteligencia Artificial	290
	II.2. La brecha digital y la inclusión en las ciudades inteligentes	298
III.	CONCLUSIONES.....	309
IV.	BIBLIOGRAFÍA.....	310

Regulación europea de la inteligencia artificial 313

SUSANA E. CASTILLO RAMOS-BOSSINI

I.	INTRODUCCIÓN.....	313
II.	LA REGULACIÓN EUROPEA DE LA IA: ANTECEDENTES Y FUTURO REGLAMENTO DE INTELIGENCIA ARTIFICIAL.....	319
	II.1. Primeros pasos en la regulación de la IA en el ámbito de la UE	319
	II.2. La propuesta de Reglamento de Inteligencia Artificial	323
	II.2.1 <i>Sistemas IA prohibidos</i>	325
	II.2.2 <i>Sistemas IA de alto riesgo</i>	327
	II.2.3 <i>Códigos de Conducta y sistemas IA de bajo o mínimo riesgo</i>	330
III.	RIESGOS Y RETOS DE LA IA.....	331
IV.	CONCLUSIONES	335
V.	BIBLIOGRAFÍA.....	337

Los algoritmos en la función administrativa 339

ÓSCAR CORTÉS ABAD

I.	INTRODUCCIÓN.....	339
II.	UNA REVISIÓN SOBRE LA INFLUENCIA RECIENTE DE LA TECNOLOGÍA EN LA REFORMA ADMINISTRATIVA	341
	II.1. Tecnologías web y nueva gestión pública	341
	II.2. Tecnologías sociales y gobierno abierto	343
	II.3. Inteligencia artificial, ¿una nueva inteligencia aplicada al gobierno?	344
III.	LA VARIEDAD DE INTELIGENCIAS Y LOS TRADE OFFS QUE PLANTEAN SU USO EN LA FUNCIÓN ADMINISTRATIVA	347
	III.1. Modelos de Administración algorítmica	347
	III.2. Los tradeoffs en el uso de la IA en la función administrativa	350
IV.	ÁMBITOS DE INFLUENCIA DE LOS ALGORITMOS EN LA FUNCIÓN ADMINISTRATIVA	354
	IV.1. La influencia sobre el procedimiento administrativo	354
	IV.2. La influencia sobre la función pública	361
	IV.3. La influencia sobre la transparencia y buen gobierno	364
V.	CONCLUSIONES	367
VI.	REFERENCIAS BIBLIOGRÁFICAS	369

Propuesta de regulación de una política de uso del teléfono móvil del empleado público..... 373

CAROLINA SERRANO FALCÓN

I.	LA PROPUESTA: JUSTIFICACIÓN, UBICACIÓN NORMATIVA Y REDACCIÓN DEL PRECEPTO.....	373
	I.1. Justificación	373
	I.2. Ubicación normativa	375
	I.3. Redacción del precepto	376
II.	FUNDAMENTACIÓN DE LA PROPUESTA QUE SE PRESENTA	377
	II.1. El concepto de dispositivo móvil y de empleado público	377
	II.2. La previa audiencia de los representantes de los trabajadores	378
	II.3. La finalidad preventiva y unificadora de la propuesta	378
	II.4. La necesidad de informar y formar al empleado público sobre el contenido de la política de uso de su dispositivo móvil	380
	II.5. El uso profesional del teléfono móvil	380
	II.6. Las consecuencias jurídicas de un uso inadecuado en el entorno de trabajo	396
III.	CONCLUSIONES	398
IV.	BIBLIOGRAFÍA	398
V.	INFORMES, NOTICIAS, BLOGS.....	399

El Metaverso: necesidad de un ordenamiento jurídico *ad hoc* en materia administrativa y de derechos fundamentales en Latinoamérica 401

MIRKO A. MALDONADO-MELÉNDEZ

I.	INTRODUCCIÓN.....	402
II.	EL METAVERSO, UN ECOSISTEMA VIRTUAL EN PLENO DESARROLLO Y EXPANSIÓN: BREVE ANÁLISIS DE ALGUNAS CUESTIONES PROBLEMÁTICAS EN TORNO A SU USO	405
	II.1. ¿Metaconceptos o Metanoción?: difícil encaje legal del Metaverso	409
III.	LA FUNCIÓN DEL DERECHO COMO REGULADOR DE LAS ACTUACIONES AL INTERIOR DEL METAVERSO: ¿UNA CAMISA DE FUERZA O UN GARANTE DE DERECHOS?	412
IV.	CUESTIONES PROBLEMÁTICAS DENTRO DEL METAVERSO: DESDE LA PROTECCIÓN DE DATOS PERSONALES HASTA LA RESOLUCIÓN DE CONFLICTOS	415
V.	EL METAVERSO Y LA INTELIGENCIA ARTIFICIAL EN LOS ORDENAMIENTOS JURÍDICOS EN LATAM: EL ESTADO DE LA CUESTIÓN ACTUAL Y LAS PROPUESTAS DE UNA REGULACIÓN AD HOC CON ENFOQUE EN LA PROTECCIÓN DE LOS DERECHOS DE LAS PERSONAS	417
	V.1. Derechos y Garantías fundamentales del ciudadano digital en LATAM: Breve aproximación a sus sistemas jurídicos constitucionales y legales	419
	V.2. El Estado social (¿algorítmico?) de derecho en LATAM: la puerta de entrada para una regulación de la Inteligencia Artificial y el Metaverso .	423
	V.3. Una propuesta regional de regulación <i>ad hoc</i> con énfasis en la protección de derechos fundamentales en LATAM	434
VI.	CONCLUSIONES	439
VII.	REFERENCIAS BIBLIOGRÁFICAS	441

Los derechos fundamentales de los empleados públicos en la era digital 447

BELÉN DEL MAR LÓPEZ INSUA

I.	EVOLUCIÓN DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN	447
II.	CUARTA REVOLUCIÓN TECNOLÓGICA E IMPACTO DE LAS MEDIDAS EN LAS EMPRESAS	452
	II.1. La digitalización del empleo público: transformaciones internas y Plan de digitalización 2021-2025	456
	II.2. ¿Avance o retroceso en la regulación de los derechos fundamentales de los empleados públicos?	458
III.	LOS DERECHOS FUNDAMENTALES A LA INTIMIDAD Y A LA IMAGEN DEL EMPLEADO PÚBLICO ANTE LOS RETOS DE LA DIGITALIZACIÓN	460

III.1.	El derecho a la intimidad en relación con otros derechos fundamentales	463
III.2.	Big datos y protección de datos biométricos: el Reglamento General de Protección de Datos a examen	471
IV.	SALUD LABORAL, TELETRABAJO Y DERECHO A LA DESCONEXIÓN DIGITAL	482
IV.1.	El derecho a la desconexión digital de los empleados públicos	486
IV.2.	Marco regulador del derecho a la desconexión digital: la Ley Orgánica 3/2018 de protección de datos personales y la Ley 10/2021 de trabajo a distancia	490
V.	BIBLIOGRAFÍA	496

Régimen de relación de los ciudadanos en una administración digital: notificaciones electrónicas y cita previa 501

JUAN JOSÉ LAVILLA RUBIRA

I.	INTRODUCCIÓN	501
II.	LAS NOTIFICACIONES ELECTRÓNICAS	502
II.1.	Evolución del régimen jurídico de las notificaciones electrónicas	502
II.2.	Principios generales en materia de notificaciones electrónicas	504
II.3.	Supuestos de notificación electrónica	506
II.4.	Forma de las notificaciones electrónicas	516
II.5.	Momento en el que se entienden practicadas las notificaciones electrónicas	519
II.6.	El aviso de la puesta a disposición de la notificación electrónica	522
III.	LA CITA PREVIA	524
III.1.	Situación existente en relación con la cita previa	524
III.2.	Valoración jurídica de la situación existente en relación con la cita previa	526
IV.	BIBLIOGRAFÍA	527

Los derechos fundamentales de los empleados públicos en la era digital

BELÉN DEL MAR LÓPEZ INSUA

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

SUMARIO: I. EVOLUCIÓN DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN. II. CUARTA REVOLUCIÓN TECNOLÓGICA E IMPACTO DE LAS MEDIDAS EN LAS EMPRESAS. II.1. La digitalización del empleo público: transformaciones internas y Plan de digitalización 2021-2025. II.2. ¿Avance o retroceso en la regulación de los derechos fundamentales de los empleados públicos? III. LOS DERECHOS FUNDAMENTALES A LA INTIMIDAD Y A LA IMAGEN DEL EMPLEADO PÚBLICO ANTE LOS RETOS DE LA DIGITALIZACIÓN. III.1. El derecho a la intimidad en relación con otros derechos fundamentales. III.2. Big datos y protección de datos biométricos: el Reglamento General de Protección de Datos a examen. III.2.1. Análisis comparado: la sentencia del Tribunal de Justicia de la Unión Europea de 30 de marzo de 2023 (asunto C-34/21). III.2.2. Biométrica y datos personales en la Ley de Protección de Datos. La interpretación de los tribunales europeos a la luz del Reglamento General de Protección de Datos. IV. SALUD LABORAL, TELETRABAJO Y DERECHO A LA DESCONEXIÓN DIGITAL. IV.1. El derecho a la desconexión digital de los empleados públicos. IV.2. Marco regulador del derecho a la desconexión digital: la Ley Orgánica 3/2018 de protección de datos personales y la Ley 10/2021 de trabajo a distancia. V. BIBLIOGRAFÍA.

I. EVOLUCIÓN DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

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 *iustlaboralista*. 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 (públicas y privadas), lo que ha provocado un importante cambio de mentalidad y una transformación de los modos de desempeño de la actividad profesional². 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. Lo cual abre las puertas a los empresarios a que sospechen, ante el miedo por una posible caída de la

¹ Mercader Uguina, J.R (2002): *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Valladolid: Lex Nova, p. 49.

² Sempere Navarro, A.V y San Martín Mazzucconi, C (2002): *Nuevas Tecnologías y Relaciones Laborales*, Navarra: Aranzadi, p.31. Sánchez Torres, E (2005): “El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley, p.107.

³ López-Barajas Perea, I (2011): *La intervención de las comunicaciones electrónicas*, Madrid: La Ley, p. 21.

⁴ Segoviano Astaburuaga, M.L (2004): “El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores”, *Revista Jurídica de Castilla y León*, nº 2, p. 149.

⁵ Sánchez Torres, E (2005): “El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley, p.108.

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 extra-laboral 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 bloqueos; *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

⁶ Segoviano Astaburuaga, M.L (2004): “El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores”, *Revista Jurídica de Castilla y León*, nº 2, p.149.

⁷ Fernández Collados, M.B (2020): “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*, Nº57, pp. 324-325.

empresarial (artículo 38 de la Constitución Española -CE-) y, de otro lado, los derechos fundamentales (Capítulo II, sección 1ª 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.

El vigente Real Decreto Legislativo 5/2015, de 30 de octubre por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (en adelante EBEP) 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 obje-

⁸ López Insua, B.M (2014): “Derecho fundamental a la intimidad del trabajador y poderes empresariales”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, Número 38, pp. 4-15.

⁹ Gómez Sanchidrian, D (2012): “Las nuevas tecnologías en las relaciones laborales: Control empresarial del correo electrónico y de Internet”, *Noticias Jurídicas*, Noviembre de 2012, p.1.

¹⁰ Goñi Sein, J.L (1988): *El respeto a la esfera privada del trabajador*, Madrid, Civitas, pp. 21-31.

tivo 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". Derecho que se hace extensible, igualmente, a los empleados públicos.

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 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

¹¹ Monereo Pérez, J.L y López Insua, B.M (2014): "El control empresarial del correo electrónico tras la STC 170/2013", *Aranzadi Social- Revista Doctrinal*, Número 11, p.240.

¹² Rapp, L (2000): "*Secret de correspondances et courriers électroniques*", Dalloz, n° 41, pp.3-5.

¹³ Goñi Sein, J.L (1988): *El respeto a la esfera privada del trabajador*, Madrid, Civitas, pp. 28-29.

¹⁴ Rodríguez Lainz, J.L (2010): "Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: derecho primario", *Diario La Ley*, N° 7351, p.2.

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 seña 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. CUARTA REVOLUCIÓN TECNOLÓGICA E IMPACTO DE LAS MEDIDAS EN LAS EMPRESAS

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 físicos, digitales y biológi-

cos. 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 Iot, 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 Trabajo, 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 cotidianidad 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 ajena¹⁵. Como en toda revolución tecnológica, la Industria 4.0 ha provocado una destrucción de empleos¹⁶, a la par de un surgimiento de nuevas oportunidades de negocio antes insospechadas, siendo un

¹⁵ López Insua, B.M (2018): “Trabajo decente y prestaciones ante situaciones de necesidad (I): Incapacidad para trabajar”, en VV.AA., MONEREO PÉREZ, J.L; GORELLI HERNÁNDEZ, J Y DE VAL TENA, Á.L (Diris) y LÓPEZ INSUA, B.M (Coord), *El trabajo decente*, Granada, Comares. Colección Trabajo y Seguridad Social nº111.

¹⁶ Rodríguez Escanciano, S y Álvarez Cuesta, H (2019): *Trabajo autónomo y trabajo por cuenta ajena: nuevas formas de precariedad laboral*, Albacete: Bomarzo.

claro ejemplo de nuestros tiempos el de las *youtubers* e *influencers* auspiciados al fragor de las redes sociales¹⁷.

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 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 trabajadores¹⁸ que son expuestos a dichos dispositivos¹⁹.

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 Trabajo²⁰. 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 trabajo²¹. Lo que, irremediablemente, provocará un efecto negativo sobre los derechos de los trabajadores.

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.

¹⁷ Fernández Collados, M.B (2020): “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*, N°57, p.326.

¹⁸ Monereo Pérez, J.L (2020): *La dignidad del trabajador. Dignidad de la persona en el sistema de Relaciones Laborales*, Murcia: Laborum.

¹⁹ Marín Malo, M (2020): “La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente”, *Labos*, Vol.1, N°1, p.111.

²⁰ Mercader Uguina, J. R (2017): *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia: Tirant lo Blanch, p.613.

²¹ Rodríguez Escanciano, S y Álvarez Cuesta, H (2019): *Trabajo autónomo y trabajo por cuenta ajena: nuevas formas de precariedad laboral*, Albacete: Bomarzo.

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 ajenidad 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 empresa²². Empero, todo ese debate doctrinal y jurisprudencial ha quedado zanjado 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 Estatuto de los Trabajadores una nueva disposición adicional 23^a. En particular, esta disposición presume ahora la laboralidad en el ámbito de las plataformas de

²² Monereo Pérez, J.L y López Insua, B.M (2021): “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”, *Anuario de 2020 de Jurisprudencia Laboral (Estudio de 100 casos relevantes*, Madrid: BOE, pp. 415-430.

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 Trabajo²³, sino que además implique a los representantes de los trabajadores.

El ámbito público no ha sido indiferente a esta revolución tecnológica, de hecho, ha debido, poco a poco, adaptarse. La digitalización de las Administraciones Públicas ya estaba prevista con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en donde, de una manera generalizada se han implantados los medios electrónicos en la gestión pública. No obstante, lo más olvidado en esas innovaciones tecnológicas radica en el respecto a los derechos y condiciones de trabajo de los empleados públicos, pues los derechos a la salud y al descanso de los trabajadores ha quedado a expensas del alcance del poder de dirección de las distintas Administraciones Públicas.

II.1. La digitalización del empleo público: transformaciones internas y Plan de digitalización 2021-2025

La digitalización del empleo público sigue, desde hace años, su auge en España. Previamente, en Francia el *Centre de recherche pour l'étude et l'observation des conditions de vie* (CREDOC) reflejó la necesidad de impulsar e implantar las

²³ Monereo Pérez, J.L y López Insua, B.M (2021): “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”, *Anuario de 2020 de Jurisprudencia Laboral (Estudio de 100 casos relevantes)*, Madrid: BOE, pp.415-430.

nuevas tecnologías en las distintas Administraciones Públicas ya que, como reflejan las estadísticas, el fenómeno de la digitalización optimiza el desempeño de la actividad profesional, al tiempo que agiliza los trámites burocráticos que los ciudadanos deben realizar.

España ha hecho una gran inversión en digitalizar y modernidad las Administraciones públicas. De hecho, la nación española se ha situado ya en la segunda posición, tal y como indica el Índice de Digitalización de la Economía y la Sociedad (DESI) en 2019. Pese a los avances, lo cierto es que subsisten aún carencias que dificultan el acceso a las políticas, ayudas y servicios públicos de las Administraciones por parte de algunos colectivos, sobre todo, los más vulnerables. De igual modo, el acceso de las empresas a los procedimientos digitales es aún dificultoso, en algunos casos, sobre todo en el caso de las PYMEs.

Lo cierto es que la situación de pandemia originada por el Covid-19 ha sido la que más ha alertado a la nación española de la necesidad de adoptar medidas para desarrollar una Administración digital que pueda responder a las necesidades de los ciudadanos. Es por ello que, a través de la Agenda España Digital 2025 se tratan de solventar muchas de las carencias y retrasos originados (por ejemplo: mayor transparencia, eliminación de trabas administrativas a través de la automatización de la gestión, mayor orientación a la personalización de los servicios... etcétera). Son tres los ejes principales sobre los que se estructura esta agenda, a saber: Eje 1. “Transformación digital de la Administración General del Estado”; Eje 2. “Proyectos de alto impacto en la digitalización del Sector Público” y Eje 3. “Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública, Comunidades Autónomas y Entidades Locales”.

La digitalización del empleo público está afectando desde una doble dirección, de un modo, al modo de proceder de los ciudadanos y, de otro, en la forma de trabajar de los empleados públicos y de quienes ofertan sus servicios. Ya, incluso, las mismas leyes 39/2015 y 40/2015, establecer que ciertos trámites deberán gestionarse telemáticamente cuando se trate, por ejemplo: de renovar el documento de identidad, tramitar facturas, ingresos, dar de alta o baja a trabajadores... etcétera.

A principios del año 2023, por ejemplo, salió publicado el Real Decreto 1060/2022, de 27 de diciembre, por el que se modifica el conocido Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de duración. Y justo en esta norma se introdujo la digitalización de los partes médicos de baja, alta y confirmación

de la baja de los trabajadores. La experiencia de lo ocurrido durante la pandemia del COVID-19, así como el avanzado desarrollo de los sistemas informáticos (puestos en funcionamiento, entre las Administraciones Públicas, tras las Leyes 39/2015 y 40/2015, ambas de 1 de octubre) evidencian la necesidad de modificar estos engorrosos trámites burocráticos. Se busca así evitar las consecuencias gravosas que para las personas trabajadoras supone todo este esquema, lo cual resulta congruente con la misma naturaleza de la prestación por incapacidad temporal²⁴.

Ciertamente, hace años que la Administración Pública utiliza los sistemas informáticos para agilizar y mejorar la relación con sus empleados, sin embargo, esta práctica no se trasladado -hasta ahora- a los procesos de baja por incapacidad temporal por razones que desconocemos. De igual modo, sorprende que tampoco se haya hecho extensible a otros procesos de baja, como son los derivados de los periodos de inactividad durante el riesgo durante el embarazo, lactancia, nacimiento de hijo... etcétera.

II.2. ¿Avance o retroceso en la regulación de los derechos fundamentales de los empleados públicos?

La transformación interna del empleo en las Administraciones Públicas pasa por la digitalización de todas las transacciones y mecanismos procedimentales, lo que no sólo agiliza y optimiza el desempeño de la actividad profesional, sino que al tiempo favorece el medio ambiente y reduce el tiempo de trabajo²⁵. Este ahorro permitirá dedicar más tiempo a tareas encaminadas a incrementar el valor del servicio público prestado pero, también, provocará la reducción de las plantillas de personal. Esta inevitable reducción de puestos de trabajo debe coexistir, paradójicamente, con el hecho de que sólo un tercio de las Administraciones Públicas dispone de personal propio especializado en digitalización y deben recurrir a personal externo o a empresas especializadas para poner en marcha dicha tarea²⁶.

Aparte, el reto de la digitalización exige no sólo implantar mecanismos adaptados, sino más aún impulsar nuevas estrategias de gestión personal. En

²⁴ López Insua, B.M (2023): *La garantía de los derechos sociales fundamentales en la era digital*, Granada: Comares.

²⁵ Marín Alonso, I (2020): "Digitalización e innovación tecnológica en la Administración Pública: la necesaria redefinición de los derechos de los empleados públicos", *Revista Temas Laborales*, N°151, p.383.

²⁶ <https://www.observatorio-empresas.vodafone.es/>

efecto, la estabilización de todo el personal (interino y temporal) exigirá de una planificación estratégica con vistas a la tecnificación, polivalencia y desarrollo de competencias acordes a los sistemas de promoción y mantenimiento de sistemas de selección personal²⁷.

Los empleados públicos están obligados a desarrollar funciones digitales, tal y como indica el artículo 7.3 del EBEP): "... las Administraciones Públicas podrán asignar a su personal funciones, tareas o responsabilidades distintas a las correspondientes al puesto de trabajo que desempeñen, siempre que resulten adecuados a su clasificación, grado o categoría, cuando las necesidades del servicio lo justifiquen", siendo falta disciplinaria muy grave "el notorio incumplimiento de las funciones esenciales inherentes al puesto de trabajo o funciones encomendadas" (art. 95 letra g) del EBEP) o "la desobediencia abierta a las órdenes o instrucciones de un superior, salvo que constituyan infracción manifiesta del Ordenamiento jurídico" (artículo 95 letra i) del EBEP). Justo, en este punto, se plantean dudas en cuanto a los derechos y deberes que indica el EBEP al hilo de la digitalización de las relaciones profesionales, por ejemplo, en lo que respecta al uso de la firma digital. Se trata éste de un derecho-deber que recoge el artículo 14 del EBEP y que no ha recibido un tratamiento jurídico adecuado en cuanto que revela la identidad del trabajador²⁸.

En cualquier caso, la utilización masiva de tecnología implica que el trabajo de los empleados públicos debe desempeñarse de manera distinta a la tradicional o la que, hasta hace unos años, se empleaba, pues ahora prima la gestión de datos para poder desempeñar una tarea. Ello requiere, por un lado, la adquisición de determinadas habilidades y competencias por el empleado público y su constante renovación y, por otro lado, favorece la realización del trabajo en cualquier tiempo y lugar que permita conectarse a la red, dando lugar a que el trabajo a distancia adquiera un atractivo importante para un elevado número de empleados públicos -sobre todo, de sexo femenino en cuanto facilita la conciliación de la vida personal y familiar-, haciendo palpable la porosidad de la frontera entre trabajo y vida privada de los empleados públicos que veremos más adelante²⁹. Al tiempo, los problemas de falta de

²⁷ Marín Alonso, I (2020): "Digitalización e innovación tecnológica en la Administración Pública: la necesaria redefinición de los derechos de los empleados públicos", *Revista Temas Laborales*, N°151, p.383.

²⁸ Marín Alonso, I (2020): "Digitalización e innovación tecnológica en la Administración Pública: la necesaria redefinición de los derechos de los empleados públicos", *Revista Temas Laborales*, N°151, p.384.

²⁹ Alemán Páez, F (2016): "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi travail n° 2016-1088", *Trabajo y Derecho* n° 30, p.12.

intimidad, conciliación de la vida laboral y familiar y salud se manifiestan, al igual que ya lo hacen en el ámbito privado, en el sector público. Y es que, al término, el tema de la digitalización no sólo ofrece ventajas, sino que también esconde un lado oscuro en donde las distintas Administraciones Públicas habrán de adoptar medidas.

III. LOS DERECHOS FUNDAMENTALES A LA INTIMIDAD Y A LA IMAGEN DEL EMPLEADO PÚBLICO ANTE LOS RETOS DE LA DIGITALIZACIÓN

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 misma³⁰. Por lo que de acuerdo con esta idea, los derechos fundamentales 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

³⁰ Martín Morales, R (1995): *El régimen constitucional del secreto de las comunicaciones*, Prólogo a la obra cargo de Francisco BALAGUER CALLEJÓN, Madrid: Civitas, p.13.

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))”.

Ahora bien, como ya se ha puesto de manifiesto, existe también un poder de dirección en el ámbito de las Administraciones Públicas 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 subjetivo³¹ 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 conocimiento 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,

³¹ López Díaz, E (1996): *El Derecho al Honor y el Derecho a la Intimidad*, Madrid: Dikynson, pp.248 y siguientes.

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 Derecho³². 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 tal³³. 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)). 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 empresa³⁴. 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 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”³⁵. 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 salvaguar-

³² Pérez Luño, A. E (1995): *Derechos Humanos, Estado de Derecho y Constitución*, Madrid: Tecnos, pp.317-318.

³³ Romero Pérez, X.L (2008): “El alcance del derecho a la intimidad en la sociedad actual”, *Revista Derecho del Estado*, n° 21, p.213.

³⁴ Valdés Dal-Ré, F (2004): “La dimensión laboral de la libertad de expresión”, *Relaciones Laborales*, n° 7, p.6.

³⁵ Ichino, P (1979): *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, Milano: Giuffrè, p.52.

da de los derechos fundamentales³⁶. 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.

III.1. El derecho a la intimidad en relación con otros derechos fundamentales

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

³⁶ Véanse 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 nº 149/13, publicada en Luxemburgo a 26 de noviembre del 2013).

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 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 *Ililla 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 práctica³⁷. 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 comunicaciones³⁸.

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 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 trabajadores³⁹.

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.

³⁷ Monereo Pérez, J.L. (2009): *La protección de los derechos fundamentales. El modelo europeo*, Albacete: Bomarzo, pp.121-122.

³⁸ Segoviano Astaburuaga, M.L. (2004): “El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores”, *Revista Jurídica de Castilla y León*, n° 2, p.157.

³⁹ Sánchez Torres, E. (2005): “El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley, pp.108-109.

Las garantías que recoge el artículo 18.3 CE se extienden a todas las personas, procurando así evitar cualquier tipo de intromisión tanto por los poderes públicos como de los particulares, toda vez que la protección formal que brinda esta disposición no conoce de modulaciones ni excepciones. Aquello que queda bajo el manto protector constitucional tendrá garantizada su intangibilidad por muy trascendente o insignificante que sea el acto lesivo al derecho de la persona⁴⁰ sometida a control empresarial.

En el marco de este derecho fundamental quedarán amparadas todas las formas de comunicación privada que realizan las personas, incluidas las que operen a través de la red. Por lo que los mensajes de texto que se envían desde los teléfonos móviles o incluso desde el propio ordenador al celular, constituyen también comunicaciones protegidas por la vía del artículo 18.3 de la CE (ver la sentencia del TEDH de 16 de febrero del 2000 en el caso Amman contra Suiza (TEDH 2000/87). Todavía los mensajes de correo electrónico, que tanta discusión doctrinal y jurisprudencial han originado, se les reconocen idéntico tratamiento jurídico, pues son a fin de cuentas correspondencia interpersonal⁴¹. Tanto en uno como en otro caso, la información que puede contener esos mensajes puede ser: un texto, una voz, un sonido o una imagen, que se visualiza en la pantalla de un aparato (teléfono móvil u ordenador) y que queda registrada en el mismo (Véase, a este respecto, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 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). Publicada en el Diario Oficial de las Comunidades Europeas a fecha de 31/07/2002 (L 201/37).

La salvaguarda del derecho del artículo 18.3 CE se predica de lo comunicado, sea cual sea el dato que se hubiese comunicado a la otra parte y aun cuando su contenido sea banal o de notorio interés público (FJ 4 de la STC 7/10/2013). Es decir: "... la protección del derecho al secreto de las comunicaciones alcanza no sólo al proceso de comunicación mismo, sino también la identidad subjetiva de los comunicantes, no obstante una finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos" (STC de 4 de abril de 2002 (RTC 2002/70), de 20 de mayo de 2002

⁴⁰ Rodríguez Lainz, J.L (2011): "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas", *Diario La Ley*, nº 7689, p.2.

⁴¹ Luján Alcaráz, J (2011): "La vigilancia empresarial sobre el uso de los medios informáticos puestos a disposición de los trabajadores", en VV.AA, SÁNCHEZ TRIGUEROS, C y GONZÁLEZ DÍAZ, F.A (Directores), *Libertad de Empresa y Poder de Dirección del Empresario en las Relaciones Laborales*, Navarra: Aranzadi, p.136.

(RTC 2002/123), de 24 de marzo de 2003 (RTC 2003/56) y 5 de noviembre de 2007 (RTC 2007/230). Para que se produzca una violación del derecho del artículo 18.3 CE la interferencia debe originarse durante el proceso de comunicación y no una vez concluido éste. En ese caso, si el mensaje aún no ha sido leído por su receptor, con independencia del momento en que se encuentre el proceso de comunicación (sea escrito, almacenado en el ordenador personal, memoria del teléfono o pendiente de ser enviado y recibido, pero aún no leído), se entenderá que hay una vulneración del secreto a las comunicaciones⁴² (STC de 30 de noviembre del 2000 (RTC 2000/292)). Por el contrario, hay autores que entienden que la comunicación habrá de entenderse finalizada cuando el receptor abra su correo, aunque no acceda al contenido material del mismo. Una vez finalizado el proceso comunicativo, siempre que el destinatario haya tenido conocimiento del contenido del mensaje enviado, cualquier injerencia posterior quedará impregnada de la protección prevista por el artículo 18.1 de la CE y no del secreto a las comunicaciones: “El destinatario podrá conservar el mensaje en su bandeja de entrada una vez abierto o simplemente descartar su apertura; pero una vez que ha tomado o podido tomar dicha opción, sin haber procedido a su borrado o eliminación, dejará de verse amparado por el impenetrable manto protector del secreto de las comunicaciones”⁴³. No obstante, la garantía del respeto a la intimidad del trabajador se extiende también a los supuestos en los se reproduzca el contenido de la información, cualquiera que sea el soporte utilizado, así como a los archivos personales y temporales que se encuentran en el ordenador. Por su parte, la sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7514) indica que: “... La aplicación de la garantía podría ser más discutible en el presente caso, pues no se trata de comunicaciones, ni de archivos personales, sino de los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet. Se trata más bien de rastros o huellas de la «navegación» en Internet y no de informaciones de carácter personal que se guardan con carácter reservado. Pero hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa. Así lo establece la sentencia de 3 de abril de 2007 del Tribunal Europeo de Derechos Humanos cuando señala que están incluidos

⁴² Martínez Martínez, R (2005): “Vida privada y tecnologías de la información en el entorno laboral”, *Revista Aranzadi de derecho y nuevas tecnologías*, n° 9, p.71. González Cuellar Serrano, N (2006): “Garantías constitucionales de la persecución penal en el entorno digital”, en VV.AA, *Derecho y Justicia Penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuellar García*, Madrid: Colex, 2006, p.206.

⁴³ Zoco Zabala, C (2010): “Interceptación de las comunicaciones electrónicas”, *Revista para el análisis del derecho (InDret)*, pp-10-13.

en la protección del artículo 8 del Convenio Europeo de derechos humanos «la información derivada del seguimiento del uso personal de Internet» y es que esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etcétera)”.

A parte de las telecomunicaciones y transmisión de información por vía electrónica, existen otras vías de comunicación como el “chat”, “foros sociales de internet” y de “mensajería instantánea” que son de difícil ubicación dentro de este esquema. El tratamiento en los dos primeros casos difiere del tercero, pues no es lo mismo que las conversaciones que produzcan por canal abierto que por un canal cerrado (sentencias del TC de 7/10/2013 y de 17 de diciembre del 2012 (BOE núm. 19 de 22 de enero del 2013)). La dificultosa labor de delimitación del ámbito de cobertura que precisa el artículo 18.3 CE sólo comprende a la mensajería que se realice por canal cerrado: “...quedando fuera de la protección constitucional aquellas formas de envío de la correspondencia que se configuran legalmente como comunicación abierta, esto es, no secreta” (STC de 17 de diciembre del 2012 (BOE núm. 19 de 22 de enero del 2013)).

Se entienden que son comunicaciones abiertas aquellas que se realizan a través de un canal del que no puede predicarse su confidencialidad, siendo de fácil acceso por parte de cualquier usuario, por ejemplo: los “chats” o “foros sociales de internet” en los que no se ofrece ningún tipo de restricción para que las conversaciones puedan ser conocidas por otras personas. Se tratan de comunicaciones públicas en las que participan simultáneamente y en tiempo real varios internautas, pudiendo su contenido ser conocido por cualquier otro sujeto que desee acceder a la misma a través de la red pública, salvo en caso de que se utilice la opción de comunicación bidireccional cerrada entre dos usuarios.

Más interesante aún resulta el tema de la “mensajería instantánea” que requiere para su uso de la instalación de un programa informático, a saber: *Messenger*, *Trillian*, *Softonic*, *Skype*, *Google Talk*...etcétera. Actualmente, las TIC han evolucionado hasta tal punto que desde un teléfono móvil con androi (incluso ahora desde el PC) se pueden mantener conversaciones entre una o más personas gracias al empleo del sistema de mensajería instantánea. En particular, desarrollan esta capacidad aplicaciones tales como: *WhatsApp*, *Line*, *ChatON*, *Hangouts*... etc, que permiten enviar y recibir mensajes de forma muy económica aprovechando internet. Además de utilizar la mensajería básica,

los usuarios pueden crear grupos y enviar entre ellos un número ilimitado de imágenes, videos y mensajes de audio.

Entiendo, a este respecto, que esta nueva fórmula de comunicación revisa los mismos patrones que el resto de sistema de “mensajería instantánea” y “SMS”. Razón por la cual debe hacerse extensible por analogía la protección constitucional que establece el artículo 18 de la Carta Magna, tutelándose desde el comienzo hasta el final los derechos a la intimidad y al secreto de las comunicaciones. Así es, por mucho que varíe la realidad social, la base del derecho debe permanecer inalterable y adaptarse a las nuevas circunstancias. De lo contrario el Derecho se verá abocado a la caducidad y a su desaparición.

En este hilo de consideraciones cabe entrar ahora en el terreno del correo electrónico. Encontramos, al igual que en el caso anterior, dos posiciones enfrentadas: de un lado, la de aquellos que opinan que los mensajes de correo electrónico habrá de reconocérsele el mismo tratamiento que a las comunicaciones interpersonales que ampara el artículo 18.3 CE y, de otro lado, la de los que piensan que sí las conversaciones que se efectúan a través de email son por un canal abierto a la inspección y control del empresario (para ello habrá que examinar lo dispuesto por el Convenio Colectivo y contrato de trabajo), quedarán fuera de la protección constitucional del respeto al secreto a las comunicaciones y a la intimidad. En ésta última línea caminan las sentencias del TC de 7/10/2013 y del Juzgado de lo Social de Palma de Mallorca nº291/2019, de 30 de agosto de 2019.

Siguiendo la teoría del Constitucional, cabe entender que el ordenador de empresa, al igual que el teléfono móvil profesional, constituyen elementos de trabajo que son financiados a través del patrimonio empresarial, por lo que, si en el Convenio Colectivo aplicable se sanciona como falta leve el uso de los mismos para otros fines distintos a los de la prestación laboral, cabrá entender que rige pues una prohibición expresa de uso extralaboral.

En este punto, la doctrina científica y la jurisprudencia comunitaria han entendido que el correo electrónico constituye una forma de comunicación privada, protegida por el mandato que establece el artículo 8 del CEDH: “Toda persona tiene derecho al respecto de su vida privada y familiar, de su domicilio y de su correspondencia”. De igual modo, las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de “vida privada” y “correspondencia” (véase las sentencias del TEDH de 3 de abril del 2007, en el caso Copland contra Reino Unido (TEDH 2007/23); 16 de febrero del 2000, caso Amman contra Suiza (TEDH 2000/87) y 25 de junio de 1997, caso Halford contra Reino Unido (TEDH 1997/37). Realmente el término de “vida privada” no debe interpretarse de

forma restrictiva, por lo que no cabrá excluir las actividades profesionales o comerciales de dicho concepto. Protegiéndose por este derecho cualquier dato que venga implícito en la comunicación: un texto, una imagen, la identificación de los interlocutores, fecha y duración de la conversación. En el caso de las llamadas telefónicas se protege no sólo los datos relativos a los interlocutores (identificación de los mismos), sino también a la fecha y duración de las conversaciones⁴⁴.

El respeto a la vida privada no sólo protege el derecho del individuo de crear y desarrollar relaciones con sus semejantes (STEDH de 16 de febrero del 2000, caso Amman contra Suiza (TEDH 2000/87), sino también a expresar libremente sus ideas y pensamientos sin injerencias de terceros⁴⁵. Cualquier referencia del trabajador que se obtenga de la aplicación informática revista un carácter de personal, en el sentido del artículo 2 de la Ley Orgánica de Protección de Datos de Carácter Personal (BOE n° 298 de 14 de diciembre de 1999), resultando de aplicación las limitaciones que de ella deriven⁴⁶. Se consagra así un derecho fundamental que protege a los ciudadanos frente al uso torticero de la tecnología informática, limitando cualquier injerencia que pretenda controlar el flujo de información que concierne a cada persona⁴⁷. Sólo cuando esa intromisión esté permitida, ya sea porque el empresario haya obtenido una autorización judicial (en este mismo sentido, el artículo 8.2 del CEDH -que es, según el artículo 10.2 CE, canon interpretativo del artículo 18 CE-) o el consentimiento del comunicante⁴⁸, se podrá afirmar que no se ha vulnerado el secreto a las comunicaciones (artículo 18.3 CE). De lo contrario se considerará ilícita su intervención. Solamente se admite cómo única injerencia en la vida privada la que parte de las autoridades públicas, dando por supuesto que entre particulares no puede haber injerencias consentidas (artículo 8.2 del CEDH). Luego, el empresario no podrá invadir la esfera de la *privacy* de sus trabajadores.

⁴⁴ Sentencia del TEDH, caso Malone contra Reino Unido de 2 de agosto de 1984, serie A núm. 82, ap.84.

⁴⁵ Valdés Dal-Ré, F (2004): “La dimensión laboral de la libertad de expresión”, *Relaciones Laborales*, n° 7, 225.

⁴⁶ Martínez Fons, D (2005): “El control empresarial del uso de las nuevas tecnologías en la empresa”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley, p.200.

⁴⁷ Ávila Rodríguez, C (2012): “Artículo 8. Derecho a la protección de datos de carácter personal”, en VV.AA, MONEREO ATIENZA, C y MONEREO PÉREZ, J.L (Dirección y Coordinación): *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea*, Granada: Comares, pp. 163-164.

⁴⁸ Martínez Martínez, R (2005): “Vida privada y tecnologías de la información en el entorno laboral”, *Revista Aranzadi de derecho y nuevas tecnologías*, n° 9, p.77.

III.2. Big datos y protección de datos biométricos: el Reglamento General de Protección de Datos a examen

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 procesar. A 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”. 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 obtenidos 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 mantiene 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 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 tecnológica.

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 otro.

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

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).

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 datos⁴⁹, 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 Datos indica que, a la hora de evaluar y determinar el riesgo 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

⁴⁹ 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>

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 35.3º 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.

III.2.1. Análisis comparado: la sentencia del Tribunal de Justicia de la Unión Europea de 30 de marzo de 2023 (asunto C-34/21)

Durante el año 2020, momento en el que se declaró a nivel mundial la pandemia del COVID-19, el Ministro de Educación y Cultura del Estado Federado de Hesse (Alemania) estableció el marco jurídico y organizativo de la enseñanza escolar (en centros públicos) virtuales, estableciendo, en particular, la posibilidad de que los alumnos que no pudieran estar presentes en clase asistieran en directo a las clases por videoconferencia. A 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.

Una de las cuestiones que recogía el artículo 23 de la *Hessisches Datenschutz und Informationsfreiheitsgesetz* (Ley de Protección de Datos y Libertad de

Información del Estado Federado de Hesse), de 3 de mayo de 2018, establece que “Los datos personales de los trabajadores pueden ser tratados a efectos de la relación laboral si es necesario para la decisión sobre el establecimiento de una relación laboral o, tras el establecimiento de la relación laboral, para su aplicación, rescisión o resolución, así como para la aplicación de medidas internas de planificación, organización, de naturaleza social o de personal...”. Y, todo ello, a fin de garantizar el buen funcionamiento de la organización. De acuerdo con esta idea, el apartado 3 del mencionado artículo 23 admite, prescindir del consentimiento del trabajador en el tratamiento de sus datos personales, cuando sea necesario “...cumplir obligaciones jurídicas derivadas del Derecho del trabajo, del Derecho de la seguridad social y de la protección social...”.

Aplicando la mencionada normativa, el Ministerio de Educación y Cultura del Estado Federado de Hesse censuró 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. A raíz de esta decisión, 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 (el *Verwaltungsgericht Wiesbaden*) que conoce 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 datos, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral⁵⁰. Ahora bien, dicho órgano jurisdiccional alberga dudas en cuanto a la compatibilidad de dicha normativa con las exigencias impuestas por el artículo 88, apartado 2, del Reglamento General de Protección de Datos. Por todo ello, el órgano jurisdiccional de

⁵⁰ En virtud del artículo 88, apartado 1, del RGPD, que constituye una cláusula de apertura, 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.

lo contencioso-administrativo decidió presentar dos cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea, a saber:

“1) ¿Debe interpretarse el artículo 88, apartado 1, del [RGPD] en el sentido de que, para que una disposición legislativa constituya una norma más específica 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 los efectos del citado artículo 88, apartado 1, del [RGPD], debe satisfacer las exigencias impuestas por el artículo 88, apartado 2, del [RGPD] en relación con tales disposiciones?

2) ¿Puede seguir aplicándose, así y todo, una norma nacional cuando resulte claro que no satisface las exigencias impuestas por el artículo 88, apartado 2, del [RGPD]?”.

III.2.2. Biométrica y datos personales en la Ley de Protección de Datos. La interpretación de los tribunales europeos a la luz del Reglamento General de Protección de Datos

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”⁵¹.

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 sentencia del Tribunal de Justicia de la Unión Europea de 30 de marzo de 2023 (en el asunto C-34/21) acabará declarando que una normativa nacional no puede constituir una “norma más específica”, a los efectos del apartado 1 del artículo 88, apartado 1, del Reglamento General de Protección de Datos, en caso de que no cumpla las condiciones impuestas en el apartado 2 del referido artículo. Además, el Tribunal de Justicia precisa que la aplicación de disposiciones nacionales adoptadas para garantizar la protección de los derechos y libertades de los trabajadores por lo que se refiere al tratamiento de sus datos personales en el ámbito laboral deberá excluirse cuando esas disposicio-

⁵¹ López Insua, B.M (2023): *La garantía de los derechos sociales fundamentales en la era digital*, Granada: Comares.

nes no respeten las condiciones y los límites establecidos por el citado artículo 88, apartados 1 y 2, del RGPD, a menos que dichas disposiciones constituyan una base jurídica para el tratamiento contemplada en otro artículo del RGPD que cumple con las exigencias establecidas en este.

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.

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, la cuestión más litigiosa sobrevuela en torno a la figura del “consentimiento”. ¿Resulta necesario recabar el consentimiento expreso del trabajador/s afectados en todos los casos? Sobre esta cuestión 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) otorga una interpretación bastante clara y garantista.

En primer lugar, el TJUE señala que el tratamiento de datos personales de docentes, en particular, la imagen de los mismos durante la retransmisión en directo por videoconferencia de las clases de enseñanza pública que imparten está comprendido en el ámbito de aplicación material del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y, a continuación, precisa que dicho tratamiento de datos personales de docentes que, en cuanto empleados o funcionarios, forman parte del servicio público del estado federado de Hesse, está comprendido dentro del ámbito de aplicación personal del artículo 88 del RGPD, que se refiere al tratamiento de datos personales de los trabajadores en el ámbito laboral. Partiendo de esta base, cabe analizar entonces la normativa nacional del Estado alemán para ver si es contraria al RGPD.

En segundo lugar, el Alto Tribunal Europeo analiza e interpreta la previsión recogida en el artículo 88, apartado 1 del RGPD y si, ateniendo a los hechos controvertidos, se cumplen con las condiciones recogidas por el aparta-

do segundo del mencionado artículo. Todo ello, en relación a la “norma más específica” que publica la nación alemana.

Indica el Tribunal de Justicia, acerca del uso de la expresión «más específicas» que, de acuerdo con el tenor literal del artículo 88, apartado 1, del RGPD, se desprende que las normas a las que se refiere esta disposición deben tener un contenido normativo propio del ámbito regulado, distinto de las reglas generales de dicho Reglamento. Asimismo, se desprende del apartado 2 del artículo 88 del RGPD, cuál es el margen de apreciación que los Estados miembros disponen para establecer «normas más específicas» en virtud del apartado 1 de dicho artículo. Así pues, el Tribunal de Justicia considera, por una parte, que tales normas no pueden limitarse a reiterar las disposiciones del referido Reglamento, estableciendo las condiciones de licitud del tratamiento de datos personales y los principios de dicho tratamiento⁵², o remitir a esas condiciones y principios. Las mentadas normas deben tener por objeto la protección de los derechos y libertades de los trabajadores en relación con el tratamiento de sus datos e incluir medidas adecuadas y específicas destinadas a proteger la dignidad humana, los intereses legítimos y los derechos fundamentales de los interesados, de lo contrario, se considerarán discriminatorias. Por otra parte, debe prestarse especial atención a la transparencia del tratamiento, a la transferencia de datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta, y a los sistemas de supervisión en el lugar de trabajo. Por consiguiente, para que una norma de Derecho pueda ser calificada de «norma más específica», a los efectos del apartado 1 del artículo 88 del RGPD, debe cumplir las condiciones impuestas en el apartado 2 del referido artículo.

En tercer lugar, el Tribunal de Justicia de la Unión Europea aclara las consecuencias que deben extraerse de una declaración de incompatibilidad de las disposiciones nacionales controvertidas con las condiciones y los límites previstos en el artículo 88, apartados 1 y 2, del RGPD.

Nuevamente, el TJUE recuerda aquí que será el órgano jurisdiccional remitente el único competente para interpretar el Derecho nacional y apreciar, si las disposiciones nacionales controvertidas, respetan las condiciones y los límites establecidos en el artículo 88 del RGPD. No obstante, el Tribunal de Justicia 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

⁵² Véanse los artículos 5 y 6 del RGPD.

ya establecida en el RGPD, sin añadir una norma más específica en el sentido del artículo 88, apartado 1, de dicho Reglamento. Por lo que, al no mejorar, ahondar o completar en el contenido que establece el Reglamento (UE) 2016/679⁵³, el juez nacional habrá de entender que dichas disposiciones no respetan las condiciones y los límites que recoge el artículo 88 del RGPD. Por lo que, claramente, no podrá aplicarse -en principio- la normativa nacional. En efecto, cabe traer a colación aquí el principio de la primacía del Derecho de la Unión. Y es que, 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.

Igualmente, el TJUE establece que pueden aplicarse a un tratamiento de datos personales –como el controvertido en el litigio principal– otras disposiciones del RGPD⁵⁴, en virtud de las cuales el tratamiento de datos personales será lícito si es necesario, respectivamente, para el cumplimiento de una obligación legal aplicable al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. En relación con esas dos hipótesis de licitud, el RGPD, por una parte, indica que el tratamiento debe basarse en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y añade, por otra parte, que la finalidad del tratamiento deberá quedar determinada en dicha base jurídica o ser necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Por todo lo expuesto, señala finalmente el TJUE que habrá de ser el juez nacional quien determine si las disposiciones nacionales relativas al tratamiento de datos personales en el ámbito laboral respetan o no las condiciones y límites recogidos por los apartados 1 y 2 del artículo 88 del RGPD. Además, deberá éste comprobar si dichas disposiciones constituyen una base jurídica contemplada en otro artículo del RGPD, que cumple las exigencias establecidas en el mismo Reglamento. Si es así, no deberá excluirse la aplicación de las disposiciones nacionales.

El fallo del TJUE en la sentencia de 30 de marzo de 2023 es concluyente: 1) “... una normativa nacional no puede constituir una «norma más específica», a los efectos del apartado 1 de dicho artículo, en caso de que no cumpla las condiciones impuestas en el apartado 2 del referido artículo” y 2) “... la aplicación de disposiciones nacionales adoptadas para garantizar la protec-

⁵³ De acuerdo con el artículo 6, apartado 1, párrafo primero, letra b) del RGPD.

⁵⁴ Se refiere aquí el TJUE al artículo 6 del RGPD.

ción de los derechos y libertades de los trabajadores en cuanto se refiere al tratamiento de sus datos personales en el ámbito laboral deberá excluirse cuando esas disposiciones no respeten las condiciones y los límites establecidos por el citado artículo 88, apartados 1 y 2, a menos que dichas disposiciones constituyan una base jurídica contemplada en el artículo 6, apartado 3, de dicho Reglamento que cumple las exigencias establecidas en este”.

IV. SALUD LABORAL, 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 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. La Administración Pública no es, en este punto, indiferente, en tanto que también habrá que adaptarse para proteger los derechos de sus empleados públicos frente a las posibles invasiones de sus vidas privada o de su salud. Y es que, el uso desproporcionado y abusivo de las nuevas tecnologías conlleva, inevitablemente, a que los trabajadores (incluidos los empleados públicos), queden abducidos y absorbidos por ese uso que han de hacer de los medios informáticos. Ya en la Ley Orgánica de Protección de Datos del año 2018 se

concibe el derecho a la llamada “desconexión digital” de los empleados públicos como un auténtico derecho individual. Y es que, a diferencia del ámbito privado en donde se habla del derecho al “descanso” y a las “vacaciones”, en el empleo público se va más allá. Lamentablemente, 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 empleado público, que ha de descansar entre jornadas (esto es lo que llamamos desconexión digital).

Llama la atención el Informe de la Consultora Roland Berger, elaborado en el mes de marzo de 2017, el cual indica que⁵⁵ los motores de la transformación digital son diferentes en el sector privado y en el público. En efecto, mientras que el primero se encuentra sometido a la demanda de los clientes, a la competencia y a la naturaleza misma de las actividades que se desarrollan, el sector público, en cambio, no está sometido a esa presión o lo hace de manera menos intensa y con variables propias en relación a cada organización administrativa. Si la generalización de las TIC ya supuso la necesidad de afrontar desafíos en el ámbito público que aún no se han hecho realidad (a saber: la formación continua, priorización del trabajo vinculado al cambio tecnológico, evaluación del desempeño vinculada a procesos automatizados...), la digitalización complica exponencialmente las dificultades anteriores al exigir el diseño e implementación de estrategias digitales que pongan en marcha la inteligencia artificial y el uso de algoritmos, la automatización, la asistencia virtual o el procesamiento de datos, etc. En todo caso, la sustitución de personas por robots u ordenadores inteligentes para realizar todo tipo de tareas -manuales o intelectuales, que, por muy complejas que sean, pueden expresarse en reglas programables a través de algoritmos es una amenaza que afecta de manera transversal a todos los sectores productivos, incluyendo, por tanto, el ámbito público.

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 con-

⁵⁵ http://www.rolanberger.com/fr/publications/pub_transformation_digitale_dans_le_secteur_public.html

tagio 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 familiar⁵⁶. 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. 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 determinados⁵⁷.

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 ga-

⁵⁶ López Insua, B.M (2017): *El principio de igualdad de género en el Derecho Social del Trabajo*, Murcia: Laborum.

⁵⁷ López Insua, B.M (2018): “Trabajo decente y prestaciones ante situaciones de necesidad (I): Incapacidad para trabajar”, en VV.AA., MONEREO PÉREZ, J.L; GORELLI HERNÁNDEZ, J Y DE VAL TENA, Á.L (Dir) y LÓPEZ INSUA, B.M (Coord), *El trabajo decente*, Granada, Comares. Colección Trabajo y Seguridad Social nº111, pp. 573-598.

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.

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.

IV.1. El derecho a la desconexión digital de los empleados públicos

Entiéndase por derecho a la desconexión digital la limitación en el uso de las tecnologías de la comunicación fuera del tiempo de trabajo, a fin de garantizar el respeto del tiempo de descanso, permisos y vacaciones o bajas por enfermedad (esto es, durante todo el tiempo que no sea de trabajo y conforme a la definición de la *Directiva 2003/88/CE*), así como a su intimidad personal y familiar.

El tema de la desconexión digital ha sido tratado varias veces, pero no ha sido hasta la Ley Orgánica 3/2018, de Protección de Datos personales cuando se ha regulado, por primera vez, en el ordenamiento jurídico español esta materia. Previamente, en los acuerdos para el Empleo y la Negociación Colectiva de los años 2015, 2016 y 2017 se había analizado sutilmente esta materia al re-

comendar que en “los convenios, especialmente los de empresa..”. se promuevan la racionalización del horario de trabajo para “mejorar la productividad y favorecer la conciliación de la vida personal y laboral”.

Empero, con la entrada en vigor de la Ley Orgánica 3/2018 se introduce en su artículo 88 el término de “desconexión digital” en el ámbito laboral, al indicar que todos “... los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar”. Para ello, “... el empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática”.

La lucha por regular esta materia trae su causa en la necesidad de garantizar el respeto a la intimidad laboral frente a las intrusiones del empresario en ejercicio de su poder de control, el cual queda incrementado gracias a las nuevas fórmulas tecnológicas y digitales⁵⁸. El derecho a la desconexión digital se ha consagrado como un derecho laboral de los trabajadores, previsto en el artículo 20 bis del ET y que pretende poner coto a los abusos derivados de la disponibilidad extraprofesional del trabajador. En esta misma línea, el artículo 14 del EBEP subraya que los empleados públicos tendrán garantizado el derecho a la “intimidad en el uso de los dispositivos digitales puestos a disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales”.

La sistematización de estos nuevos derechos recogidos en el art. 14 del EBEP resulta, sin duda, apropiada en la medida que todos los empleados públicos, en correspondencia con la naturaleza jurídica de su relación de servicio, -ya sean, laborales o funcionarios- pueden ejercitar los mencionados derechos sin necesidad de reiterarlo respecto de la titularidad y ejercicio de todas las condiciones de trabajo para cada tipo de personal. Su concepción como derecho individual no evita, sin embargo, críticas similares a las efectuadas sobre la regulación contenida en el art. 20 bis del ET, si bien, en el ámbito privado, no deja de ser palpable que la inclusión del mismo entre las

⁵⁸ Grau Pineda, C y Montesdesoca Suárez, A (2020): “Reconocer el derecho a la desconexión digital para garantizar el derecho a la intimidad personal y familiar”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, N°57, p.361.

facultades directivas del empleador parece más bien una contraprestación a la ampliación de las facultades de vigilancia y control que un derecho con entidad propia. Por otro lado, el derecho a la intimidad ante las tecnologías y el derecho a la desconexión digital no deberían limitarse, sin embargo, a los derechos de ejercicio individual sino extenderse, además, a los de ejercicio colectivo pues las tecnologías también tienen incidencia en dicho marco. En definitiva, la Ley de Protección de Datos se aplica a las relaciones laborales y funcionariales de la Administración Pública, siendo incluso una materia a negociar de manera común en las mesas de negociación colectiva conjunta del art. 36.3 del EBEP.

Por todo ello, el deber empresarial de las Administraciones Públicas a la desconexión digital se materializa en cuatro puntos básicos, a saber: 1) Limitación del uso de los medios tecnológicos en el ámbito laboral a la duración máxima de la jornada y fijada normativamente o vía convenio colectivo; 2) Elaboración de una política interna en consenso con la representación legal de las personas trabajadoras definiendo las modalidades de ejercicio del derecho a la desconexión; 3) Acciones de formación y de sensibilización del personal y directivos sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática y 4) Una organización adecuada de la jornada laboral de forma que sea compatible con la garantía del descanso en base al registro horario.

De acuerdo a todo lo expuesto, el derecho a la “desconexión digital” se configura como un derecho que protege al empleado público fuera de su tiempo de trabajo, pues queda claro que, en tiempo y horas de trabajo, éste configura como un deber del mismo. La finalidad del derecho a la “desconexión digital” no es otra que la de garantizar el derecho a no ser molestado en períodos de no trabajo (descanso, permisos, vacaciones, IT...) y facilitar, además, la conciliación de la vida personal o personal con la laboral. Es, sin embargo, la implementación del derecho el principal problema a evaluar pues, por un lado, el ejercicio de este derecho dependerá de la naturaleza de la relación entablada en el empleado y la Administración Pública (por ejemplo: alta dirección laboral o funcionarial ex art. 13 EBEP), así como del lugar de la prestación y, por otro lado, será la negociación colectiva o los acuerdos entre la Administración Pública y los representantes de los empleados públicos los que delimiten las modalidades de ejercicio del derecho y las acciones de sensibilización y formación sobre el correcto uso o, al menos, sobre el uso razonable de las herramientas tecnológicas. En todo caso, es sobre la Administración Pública sobre quien recae la obligación de poner en marcha la política de desconexión digital, previo acuerdo con los representantes de

los empleados públicos, no siendo exigible este derecho por los empleados sin la previa regulación convencional.

La falta de un desarrollo legal innovador y garantista ha sido determinante para que la “Ley 20/2021, de 9 de julio, de trabajo a distancia” refuerce las previsiones que ya establecen, de un lado, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, de otro, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Se pretende así poner fin a la enorme litigiosidad que, en sede doctrinal y jurisprudencial, origina esta ardua materia. El problema es que no quedan claros, pero tampoco se desarrollan suficientemente los límites entre el control empresarial y el respeto a la intimidad del trabajador (tanto dentro del ámbito laboral, como fuera de las horas de trabajo). Estos conflictos surgen, en la mayoría de las ocasiones, porque existe una utilización personalizada y no meramente laboral o profesional de los medios informáticos facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador ⁵⁹ –como sucede también con las conversaciones telefónicas en la empresa– y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. Por otra parte, cabe recordar que –en muchas ocasiones– los medios empleados son propiedad de la empresa, de ahí el excesivo poder de vigilancia que los empresarios efectúan sobre los trabajadores (artículo 20.3 del ET).

La eliminación de estas fronteras para el disfrute por el trabajador de su derecho a la intimidad y al descanso ha constituido, de hecho, una de las principales reivindicaciones obreras a fin de ofrecer un trabajo digno que cumpla con las notas de seguridad y dignidad⁶⁰. Para ello, la Organización Internacional del Trabajo ha venido reiterando, desde su nacimiento, en la necesidad de procurar la limitación de las jornadas de trabajo excesivas que conculcan tanto el derecho al descanso como el de conciliación de la vida laboral y familiar. Camino que ha seguido el artículo 34.1 del ET, así como las Directivas 93/104/CE del Consejo (de 23 de noviembre de 1993) y 2003/88/UE, relativa a los tiempos de ordenación del trabajo y de los periodos de des-

⁵⁹ Ortega Lozano, P (2019): *Las consecuencias jurídicas del despido: Procedencia, improcedencia y nulidad*, Murcia: Laborum.

⁶⁰ Aguilera Izquierdo, R y Cristóbal Roncero, R (2017), “Nuevas tecnologías y tiempo de trabajo: el derecho a la desconexión digital”, en VV.AA., *El futuro que queremos. Conferencia Nacional Tripartita, 28 de marzo de 2017*, Volumen 2, p.333.

canso. De igual modo, caben citar los artículos 24 de la declaración Universal de Derechos Humanos y el artículo 2 de la Carta Social Europea.

IV.2. Marco regulador del derecho a la desconexión digital: la Ley Orgánica 3/2018 de protección de datos personales y la Ley 10/2021 de trabajo a distancia

Antes de la aprobación de la Ley Orgánica 3/2018 de Protección de Datos no existía en España una normativa reguladora específica para el derecho a la desconexión digital, de ahí que la remisión debía hacerse -con carácter general- a los artículos 34, 37 y 38 del Estatuto de los Trabajadores (relativos al descanso diario, semanal o anual del trabajador). Ciertamente, el derecho al descanso se establece en nuestro ordenamiento jurídico a fin de poner coto a los excesos empresariales, procurando de este modo garantizar un derecho al trabajo decente, así como un respeto a los derechos a la intimidad y a la conciliación de la vida laboral y familiar del trabajador⁶¹. En este sentido, el debate que genera la desconexión digital no debe hacernos creer que sin su reconocimiento jurídico expreso podría este ser admisible jurídicamente. Aceptar esta premisa supondría dejar a un lado el principal motivo de nacimiento de este derecho, eso es, la interconectividad permanente del trabajador a través de las herramientas digitales⁶².

La sociedad contemporánea 4.0 se obliga a estar constantemente conectado a las nuevas tecnologías para así incrementar la competitividad y la productividad empresarial, lo que al tiempo facilita, de un lado, trabajar desde cualquier lugar y en cualquier momento, aunque también permite, de otro lado, una flexibilización en las obligaciones laborales que puede restringir en derechos laborales⁶³. Al hilo de la pandemia del COVID-19 el derecho a la desconexión digital aparece con fuerza debido a la notable absorción de espacios de la vida privada y de la salud de los trabajadores, con motivo del incremento en el empleo de las TIC's, lo que determina que el trabajador esté siempre co-

⁶¹ Gorelli Hernández, J (2018): "Trabajo decente y tiempo de trabajo", VV.AA., MONEREO PÉREZ, J.L; GORELLI HERNÁNDEZ, J Y DE VAL TENA, Á.L (Diris) y LÓPEZ INSUA, B.M (Coord): *El trabajo decente*, Granada: Comares. Colección Trabajo y Seguridad Social n°111, pp. 141-150.

⁶² Fernández Avilés, J.A (2018): "Cronoreflexión al hilo de cuestiones actuales sobre tiempo de trabajo", *Revista de Trabajo y Seguridad Social*, n°421, p.15.

⁶³ Moreno Vida, M^aN (2019): "Las facultades de control fuera de la jornada de trabajo: desconexión digital y control del trabajador", *Revistas Temas Laborales*, N°150/2019. Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos, pp. 173-175.

nectado y a disposición de la empresa. Esta realidad invita a reflexionar acerca de la incidencia directa que sobre los derechos fundamentales de los trabajadores plantea el recurso habitual y excesivo a las nuevas tecnologías⁶⁴.

Como antecedentes regulatorios, a nivel comunitario e internacional, aparece primeramente el artículo 24 de la *Declaración Universal de Derechos Humanos de 1948*, en donde se reconoce el derecho de toda persona al descanso, al disfrute del tiempo libre, y a una limitación razonable de la duración del trabajo. En segundo lugar, destaca el *Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966* que, igualmente, reconoce el derecho al disfrute de condiciones de trabajo que aseguren, en especial, el descanso, el disfrute del tiempo libre, y la limitación razonable de las horas de trabajo. Asimismo, cabe destacar en tercer lugar el derecho al descanso previsto en el artículo 31 de la Carta de los Derechos Fundamentales de la Unión Europea, de 12 de diciembre de 2007 y la Directiva 2003/88/CE del Parlamento Europeo y del Consejo de 4 de noviembre de 2003, relativa a determinados aspectos de la ordenación del tiempo de trabajo. En cuarto lugar, aparecen en materia de seguridad y salud la Directiva 89/391/CEE del Consejo, de 12 de junio de 1989, relativa a la introducción de medidas para fomentar la mejora de la seguridad y la salud de los trabajadores en el trabajo y la Directiva 91/383/CEE del Consejo, de 25 de junio, de 1991, por la que se complementan las medidas para fomentar la mejora de la seguridad y la salud en el trabajo de los trabajadores sujetos a una relación laboral de duración determinada o una relación laboral temporal. Finalmente, en lo que concierne a la conciliación de la vida laboral y familiar se presenta la Directiva (UE) 2019/1158 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el equilibrio entre la vida personal y laboral de los padres y cuidadores.

Sin embargo, el Código Civil francés fue el primero en dar carta de naturaleza a este derecho a la desconexión digital. Es por ello que en el año 2016 saliera publicada en Francia la Ley n° 2016-1088, de 8 de agosto de 2016 (conocida como “*El Khomri*”) relativa al trabajo, a la modernización del diálogo social y al aseguramiento de los recorridos profesionales. Esta ley introdujo, de forma innovadora, el derecho de todos los trabajadores a la desconexión digital para lo cual las empresas debían marcar los límites a este derecho a través de la negociación colectiva o mediante un estatuto⁶⁵. De hecho, el actual Código de Trabajo francés dispone que el empresario deberá negociar: “... la

⁶⁴ Grau Pineda, C y Montesdesoca Suárez, A (2020): “Reconocer el derecho a la desconexión digital para garantizar el derecho a la intimidad personal y familiar”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, N°57, p. 381.

⁶⁵ Trujillo Pons, F (2021): “Un estudio acerca de la eventual Directiva comunitaria sobre el derecho a la desconexión digital en el trabajo”, *Revista IusLabor 2/2021*, p. 70.

puesta en marcha de dispositivos de regulación de la utilización de los dispositivos digitales, a fin de asegurar el respeto al tiempo de descanso y vacaciones, así como su vida personal y familiar”.

En España, sin embargo, este derecho no queda normativamente regulado hasta la entrada en vigor de la Ley Orgánica 3/2018. Todos los pronunciamientos judiciales recaídos, hasta la fecha, ponen de manifiesto la necesidad de ordenar y escindir el tiempo de trabajo del descanso del trabajador.

La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales constituye un primer paso para tratar de regular este derecho a la desconexión digital, buscando así aunar los numerosos vaivenes jurisprudenciales (tanto nacionales, como europeos). Por medio del artículo 88 de esta ley se incorpora al ET un nuevo artículo 20 bis, no obstante, cabe tener en cuenta también el artículo 18 del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia. Y, asimismo, la Disposición Final decimo cuarta de la Ley Orgánica 3/2018 por la se regula el artículo 14. j) bis de la Ley del Estatuto Básico del Empleado Público.

Aparte, cabe considerar otros preceptos relevantes, a saber: el artículo 87 de la Ley Orgánica 3/2018 por la que se reconoce al empleado el derecho a la intimidad en el uso de los dispositivos digitales puestos a disposición por el empleador; el derecho la intimidad frente al uso de los dispositivos de videovigilancia y de grabación de sonidos (en el artículo 89) y a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (artículo 90). En este sentido, el artículo 18 la Ley 10/2021, de 9 de julio, de trabajo a distancia regula nuevamente el tema de la desconexión digital, al hilo de la crisis sanitaria causada por el COVID-19. Procurando, de este modo, adecuar la normativa nacional al acervo de normas internacionales, comunitarias y nacionales que integran ese «suelo social mínimo» (entre las que se encuentran, la Recomendación (UE) 2017/761 de la Comisión, de 26 de abril de 2017, sobre el pilar europeo de derechos sociales, capítulo II, la Directiva 2003/88/CE del Parlamento Europeo y del Consejo de 4 de noviembre de 2003 relativa a determinados aspectos de la ordenación del tiempo de trabajo, la Carta Social Europea, hecha en Turín de 18 de octubre de 1961, ratificada por Instrumento de 29 de abril de 1980, la Ley Orgánica 3/2018, 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la Directiva Marco 89/391/CEE del Consejo, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo y el propio texto refundido de la Ley del Estatuto de los Trabajadores. Y, finalmente, el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia). Empero, este nuevo artículo 18

de la Ley 10/2021 está siendo duramente criticado debido a que mantiene, prácticamente inalterada, la misma redacción que ya incluía el Real Decreto-ley 28/2020 y que se remite al artículo 88 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

El artículo 88 de la Ley Orgánica 3/2018 se puede analizar en tres partes que, a continuación, se exponen:

1) “Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar” (artículo 88.1). Se trata de un precepto redactado en términos muy amplios y que surge ante la necesidad de evitar que los trabajadores estén “permanentes conectados o en línea”, con el menoscabo que ello puede llegar a suponer en su salud mental o incluso en su privacidad. Por lo que se pretende así limitar los posibles abusos de los medios electrónicos fuera del horario laboral. A pesar de esta previsión, ya se han dictado algunas resoluciones relevantes que conviene comentar.

Dado que se trata de un derecho inherente a la condición de persona o de ciudadano y adscrito universalmente a todos en cuanto personas o en cuanto personas y ciudadanos, de carácter indisponible e inalienable y, además, positivado en la Carta Magna, cabe afirmar que el derecho a la desconexión digital integra el derecho a no responder a las llamadas, mensajes, correos o requerimientos empresariales recibidos fuera de la jornada de trabajo.

Ahora bien, no es sólo la Ley la que garantiza el derecho al descanso y sin intromisión de obligaciones laborales, sino que además el Tribunal Constitucional ya ha dicho que: “... *el derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*” (sentencias 94/1998, de 4 de mayo y 292/2000, de 30 de noviembre).

Por tanto, no se puede imponer a los empleados públicos la obligación de conectarse remotamente con finalidad laboral desde fuera del centro de trabajo en sus tiempos de descanso y dicho derecho es un mínimo garantizado por Ley Orgánica como desarrollo, al amparo del artículo 18.4 de la Constitución, del derecho fundamental a la intimidad personal y familiar. Ahora bien, como sostiene correctamente la recurrente, el derecho del trabajador no es incompatible con que la empresa pueda imponer la realización de actividades laborales fuera del horario ordinario, que pueden tener carácter obligatorio, salvo cuando se trate de realizar horas extraordinarias, que solamente tienen carácter obligatorio cuando así se haya pactado individual o colectivamente. Esas actividades laborales, que computan como tiempo de trabajo, pueden ser presenciales o a distancia, pero ello no altera su naturaleza.

2) El apartado 2 del artículo 88 de la Ley Orgánica 3/2018 establece que “Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores”. Una idéntica previsión se establece en segundo párrafo del artículo 18.1 de la Ley 10/2021, de 9 de julio. Ambos preceptos encomiendan a la negociación colectiva y a los representantes de los representantes de los trabajadores la elaboración de una política adecuada a este respecto. Para lo cual deberán, los representantes de los trabajadores y de los empresarios, pactar en los convenios colectivos las cláusulas que adapten las nuevas tecnologías al ámbito de las relaciones laborales. En efecto, esta idea queda una vez más remarcada en el nuevo artículo 18.2 de la Ley 10/2021, en donde en su apartado segundo se establece lo siguiente: “Los convenios o acuerdos colectivos de trabajo podrán establecer los medios y medidas adecuadas para garantizar el ejercicio efectivo del derecho a la desconexión en el trabajo a distancia y la organización adecuada de la jornada de forma que sea compatible con la garantía de tiempos de descanso”. Para ello, habrá de atenderse a la actividad concreta a realizar por los trabajadores, pudiéndose regular a través de la negociación colectiva una jornada mínima presencial en el trabajo a distancia, así como las posibles circunstancias extraordinarias y todo ello a fin de que se respete el derecho a la desconexión digital (véase la Disposición adicional primera de la Ley 10/2021, de 9 de julio, de trabajo a distancia).

3) Finalmente, el apartado 3 del artículo 88 de la Ley Orgánica 3/2018 establece que: “El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejer-

cicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas”. Más específicamente, el artículo 18.2 de la Ley 10/2021, de 9 de julio, recoge lo siguiente: “La empresa, previa audiencia de la representación legal de las personas trabajadoras, elaborará una política interna dirigida a personas trabajadoras, incluidas las que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio de la persona empleada vinculado al uso con fines laborales de herramientas tecnológicas”. Cabe entender aquí que, en defecto de regulación convencional podrán adoptarse acuerdos de empresa o directrices, siempre y cuando exista consenso entre el empresario y los representantes de los trabajadores⁶⁶. En buena medida, en estos acuerdos se tratará de llevar a cabo una política interna en materia de protección de datos que abarque un protocolo de buenas prácticas en el uso de las tecnologías y herramientas tecnológicas. A partir de estas pautas, deberá analizarse cómo debe protegerse la desconexión digital del trabajador que permita conciliar su vida personal y familiar del ámbito laboral, atendiendo a las características del puesto o de la modalidad de trabajo que se desarrolle⁶⁷.

Todas estas obligaciones empresariales deberán ser puestas en funcionamiento por las empresas y organizaciones con independencia de su actividad o tamaño. En caso contrario, el Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social (LISOS) podrá considerar, como infracción leve, los incumplimientos que afecten a obligaciones meramente formales o documentales (artículo 6.6 de la LISOS) o, como infracción muy grave, la transgresión de las normas y los límites legales o pactados en materia de jornada, trabajo nocturno, horas extraordinarias, horas complementarias, descan-

⁶⁶ Moreno Vida, M^aN (2019): “Las facultades de control fuera de la jornada de trabajo: desconexión digital y control del trabajador”, *Revistas Temas Laborales*, N^o150/2019. Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos, p. 178.

⁶⁷ Grau Pineda, C y Montesdesoca Suárez, A (2020): “Reconocer el derecho a la desconexión digital para garantizar el derecho a la intimidad personal y familiar”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, N^o57, p. 385.

sos, vacaciones, permisos y, en general, el tiempo de trabajo que protege tanto el ET, como el EBEP.

V. BIBLIOGRAFÍA

- Aguilera Izquierdo, R y Cristóbal Roncero, R (2017), “Nuevas tecnologías y tiempo de trabajo: el derecho a la desconexión digital”, en VV.AA., *El futuro que queremos. Conferencia Nacional Tripartita, 28 de marzo de 2017*, Volumen 2.
- Alemán Páez, F (2016): “El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi travail n° 2016-1088”, *Trabajo y Derecho* n° 30, p.12.
- Álvarez Del Cuvillo, A (2020), «La delimitación del derecho a la intimidad de los trabajadores en los nuevos escenarios digitales», *Revista Temas Laborales*, n°151.
- Arbonés Lapena, H.I (2013), “El acceso por el empresario al ordenador y correo electrónico del trabajador, ¿un tema resuelto?”, *Revista de Información Laboral*, n° 8.
- Ávila Rodríguez, C (2012): “Artículo 8. Derecho a la protección de datos de carácter personal”, en VV.AA, MONEREO ATIENZA, C y MONEREO PÉREZ, J.L (Dirección y Coordinación): *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea*, Granada: Comares.
- Dabin, J (2006), *El derecho subjetivo*, edición al cuidado de Monereo Pérez, J.L., Granada: Comares.
- Fernández Avilés, J.A (2018): “Cronoreflexión al hilo de cuestiones actuales sobre tiempo de trabajo”, *Revista de Trabajo y Seguridad Social*, n°421.
- Fernández Collados, M.B (2020): “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*, N°57.
- García-Perrote Escartín, I. y Mercader Uguina, J.R (2018): “El protagonismo del convenio colectivo en el nuevo reglamento de protección de datos”, *Revista de Información Laboral*, n° 6.
- Gómez Sanchidrian, D (2012): “Las nuevas tecnologías en las relaciones laborales: Control empresarial del correo electrónico y de Internet”, *Noticias Jurídicas*, Noviembre de 2012.
- González Cuellar Serrano, N (2006): “Garantías constitucionales de la persecución penal en el entorno digital”, en VV.AA, *Derecho y Justicia Penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuellar García*, Madrid: Colex, 2006.
- González González, G (2019): “Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador.

- Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”, *Aranzadi Digital*, núm. 4.
- Goñi Sein, J.L (1988): *El respeto a la esfera privada del trabajador*, Madrid, Civitas.
- Gorelli Hernández, J (2018): “Trabajo decente y tiempo de trabajo”, VV.AA., MONEREO PÉREZ, J.L; GORELLI HERNÁNDEZ, J Y DE VAL TENA, Á.L (Dir) y LÓPEZ INSUA, B.M (Coord): *El trabajo decente*, Granada: Comares. Colección Trabajo y Seguridad Social n°111.
- Grau Pineda, C y Montesdesoca Suárez, A (2020): “Reconocer el derecho a la desconexión digital para garantizar el derecho a la intimidad personal y familiar”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, N°57.
- Gude Fernández, A (2014): “La videovigilancia laboral y el derecho a la protección de datos de carácter personales”, *Revista de Derecho Político*, N°91, septiembre-diciembre.
- Guillén Catalán, R (2004): “Control o fiscalización del correo electrónico de los trabajadores por su empresa”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n° 4.
- Ichino, P (1979): *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, Milano: Giuffrè.
- López Díaz, E (1996): *El Derecho al Honor y el Derecho a la Intimidad*, Madrid: Dikynson.
- López Insua, B.M (2014): “Derecho fundamental a la intimidad del trabajador y poderes empresariales”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, Número 38.
- López Insua, B.M (2017): *El principio de igualdad de género en el Derecho Social del Trabajo*, Murcia: Laborum.
- López Insua, B.M (2018): “Fronteras entre el trabajo asalariado y el autónomo: el trabajador autónomo económicamente dependiente”, en VV.AA., Cerejeira Namora, N., Mella Méndez, L., Abrunhosa e Sousa, D., Cerejeira Namora, G y Castro Marqués, E (Edit)., *The Balance between Worker Protection and Employer Powers*, Reino Unido: Cambridge Scholar.
- López Insua, B.M (2018): “Trabajo decente y prestaciones ante situaciones de necesidad (I): Incapacidad para trabajar”, en VV.AA., MONEREO PÉREZ, J.L; GORELLI HERNÁNDEZ, J Y DE VAL TENA, Á.L (Dir) y LÓPEZ INSUA, B.M (Coord), *El trabajo decente*, Granada, Comares. Colección Trabajo y Seguridad Social n°111.
- López Insua, B.M (2021): “Derecho a la intimidad en el trabajo y nuevas tecnologías”, en VV.AA., MONEREO PÉREZ, J.L., VILA TIERNO, F., ESPÓSITO, M y PERÁN QUESADA, S (Dir) y ORTEGA LOZANO, P.G y RUIZ SANTAMARÍA, J.L: *Innovación tecnológica, cambio social y sistema de relaciones laborales*, Granada: Comares.
- López Insua, B.M (2023): *La garantía de los derechos sociales fundamentales en la era digital*, Granada: Comares.

- López-Barajas Perea, I (2011): *La intervención de las comunicaciones electrónicas*, Madrid: La Ley.
- Luján Alcaráz, J (2011): “La vigilancia empresarial sobre el uso de los medios informáticos puestos a disposición de los trabajadores”, en VV.AA, SÁNCHEZ TRIGUEROS, C y GONZÁLEZ DÍAZ, F.A (Directores), *Libertad de Empresa y Poder de Dirección del Empresario en las Relaciones Laborales*, Navarra: Aranzadi.
- Maestre Rodríguez, J (2011): “La intervención de comunicaciones electrónicas en la empresa. Comentario a la sentencia del Juzgado de lo Social de Barcelona núm. 32, de 16 de septiembre del 2002”, *Revista de Ciencias Jurídicas y Sociales*, nº 14.
- Marín Alonso, I (2020): “Digitalización e innovación tecnológica en la Administración Pública: la necesaria redefinición de los derechos de los empleados públicos”, *Revista Temas Laborales*, Nº151.
- Marín Malo, M (2020): “La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente”, *Labos*, Vol.1, Nº1.
- Martín Morales, R (1995): *El régimen constitucional del secreto de las comunicaciones*, Prólogo a la obra cargo de Francisco BALAGUER CALLEJÓN, Madrid: Civitas.
- Martínez Fons, D (2005): “El control empresarial del uso de las nuevas tecnologías en la empresa”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley.
- Martínez Martínez, R (2005): “Vida privada y tecnologías de la información en el entorno laboral”, *Revista Aranzadi de derecho y nuevas tecnologías*, nº 9.
- Mercader Uguina, J. R (2017): *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia: Tirant lo Blanch.
- Mercader Uguina, J.R (2002): *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Valladolid: Lex Nova.
- Miñarro Yanini, M (2019): “La desconexión digital en la práctica negocial: más forma que fondo en la configuración del derecho”, *Revista Trabajo y Seguridad Social. CEF*, nº440.
- Miñarro Yanini, M (2018): “Impacto del Reglamento Comunitario de Protección de Datos en las relaciones laborales: un –pretendido– “cambio cultural”, *Revista de Trabajo y Seguridad Social. CEF*, nº 423.
- Monereo Pérez, J.L y López Insua, B.M (2014): “El control empresarial del correo electrónico tras la STC 170/2013”, *Aranzadi Social- Revista Doctrinal*, Número 11.
- Monereo Pérez, J.L y López Insua, B.M (2021): “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”, *Anuario de 2020 de Jurisprudencia Laboral (Estudio de 100 casos relevantes)*, Madrid: BOE.
- Monereo Pérez, J.L y Ortega Lozano, P.G (2019): “El control empresarial del correo electrónico del trabajador”, *Revistas Temas Laborales*, Nº150/2019. Monográfico

sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos.

- Monereo Pérez, J.L (2020): *La dignidad del trabajador. Dignidad de la persona en el sistema de Relaciones Laborales*, Murcia: Laborum.
- Monereo Pérez, J.L (2009): *La protección de los derechos fundamentales. El modelo europeo*, Albacete: Bomarzo.
- Montoya Melgar A (2009): “Nuevas tecnologías y buena fe contractual (Buenos y malos usos del ordenador en la empresa)”, *Revista Relaciones Laborales*, Tomo I.
- Moreno Vida, M^aN (2019): “Las facultades de control fuera de la jornada de trabajo: desconexión digital y control del trabajador”, *Revistas Temas Laborales*, N°150/2019. Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos.
- Orozco Pardo, G (2012): “Artículo 7. Respeto de la vida privada y familiar”, en VV.AA, MONEREO ATIENZA, C y MONEREO PÉREZ, J.L (Dirección y Coordinación), *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea*, Granada: Comares.
- Ortega Lozano, P (2019): *Las consecuencias jurídicas del despido: Procedencia, improcedencia y nulidad*, Murcia: Laborum.
- Ortiz Vallejo, A (1995): *Derecho a la intimidad e informática*, Granada: Comares.
- Ortiz Fernández, M (2008): “Derecho a transmitir información sindical a los afiliados a través del correo electrónico de la empresa. Comentario a la Sentencia del Tribunal Supremo (Sala de lo Social), de 26 de noviembre del 2001”, *Datospersonales.org: Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n° 31.
- Palomeque López, M.C (1991): *Los derechos laborales en la Constitución Española*, Madrid: CEC.
- Parejo Alfonso, L (1997): “El derecho fundamental a la intimidad y sus restricciones”, en VV.AA, LÓPEZ ORTEGA, J.J (COLABORADOR), *Perfiles del Derecho Constitucional a la vida privada y familiar (Cuadernos de Derecho Judicial)*, Madrid: Consejo General del Poder Judicial.
- Pérez Gil, J (2010): “Los datos sobre localización geográfica en la investigación penal”, en VV.AA, PEDRAZ PENALVA, E (COORD), *Protección de datos y proceso penal*, Madrid: La Ley.
- Pérez Luño, A. E (1995): *Derechos Humanos, Estado de Derecho y Constitución*, Madrid: Tecnos.
- Rapp, L (2000): “*Secret de correspondances et courriers électroniques*”, *Dalloz*, n° 41.
- Rivero Lamas, J y Monereo Pérez, J.L (2012): “ARTÍCULO 20. Dirección y control de la actividad laboral”, en VV.AA, MONEREO PÉREZ, J.L (Dirección) y SERRANO FALCÓN, C (Coordinación), *El nuevo Estatuto de los Trabajadores. Estudio jurídico-sistemático del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores*, Granada: Comares.

- Rodríguez Escanciano, S y Álvarez Cuesta, H (2019): *Trabajo autónomo y trabajo por cuenta ajena: nuevas formas de precariedad laboral*, Albacete: Bomarzo.
- Rodríguez Escanciano, S (2018): “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Revista de Trabajo y Seguridad Social*, n° 423.
- Rodríguez Lainz, J.L (2010): “Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: derecho primario”, *Diario La Ley*, N° 7351.
- Rodríguez Lainz, J.L (2011): “SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas”, *Diario La Ley*, n° 7689.
- Rodríguez Ruíz, B (1998): *El secreto de las comunicaciones: tecnología e intimidad*, Madrid: McGraw Hill.
- Romero Pérez, X.L (2008): “El alcance del derecho a la intimidad en la sociedad actual”, *Revista Derecho del Estado*, n° 21.
- Sánchez Torres, E (2005): “El ejercicio de la libertad de expresión de los trabajadores a través de las nuevas tecnologías”, en VV.AA, DEL REY GUANTER, S (DIRECTOR) y LUQUE PARRA, M (COORDINADOR), *Relaciones Laborales y Nuevas Tecnologías*, Madrid: La Ley.
- Segoviano Astaburuaga, M.L (2004): “El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores”, *Revista Jurídica de Castilla y León*, n° 2.
- Sempere Navarro, A.V y San Martín Mazzucconi, C (2006): “Nuevas Tecnologías y Relaciones Laborales: una tipología jurisprudencial”, *Revista Aranzadi de derecho y nuevas tecnologías*, n° 10.
- Sempere Navarro, A.V y San Martín Mazzucconi, C (2002): *Nuevas Tecnologías y Relaciones Laborales*, Navarra: Aranzadi.
- Todoí Signes, A (2021): “Nulidad o improcedencia en caso de vulneración de derechos fundamentales en la adquisición de la prueba, pero siempre una indemnización adicional. Comentario a la Sentencia del Tribunal Constitucional 61/2021, de 15 de marzo”, *Estudios Financieros. Revista trabajo y Seguridad Social*, n°459.
- Trujillo Pons, F (2021): “Un estudio acerca de la eventual Directiva comunitaria sobre el derecho a la desconexión digital en el trabajo”, *Revista IusLabor 2/2021*.
- Valdés Dal-Ré, F (2012): “Artículo 11. La libertad de expresión e información”, en VV.AA, MONEREO ATIENZA, C y MONEREO PÉREZ, J.L (Dirección y Coordinación), *La Europa de los Derechos. Estudio sistemático de la Carta de los Derechos Fundamentales de la Unión Europea*, Granada, Comares.
- Valdés Dal-Ré, F (2004): “La dimensión laboral de la libertad de expresión”, *Relaciones Laborales*, n° 7.
- Zoco Zabala, C (2010): “Interceptación de las comunicaciones electrónicas”, *Revista para el análisis del derecho (InDret)*.