

MIGUEL RODRÍGUEZ-PIÑERO ROYO
ADRIÁN TODOLÍ SIGNES

VIGILANCIA Y CONTROL EN EL DERECHO DEL TRABAJO DIGITAL

Primera edición, 2020

1170745



THOMSON REUTERS PROVIEW eBooks

Incluye versión en digital

El editor no se hace responsable de las opiniones recogidas, comentarios y manifestaciones vertidas por los autores. La presente obra recoge exclusivamente la opinión de su autor como manifestación de su derecho de libertad de expresión.

La Editorial se opone expresamente a que cualquiera de las páginas de esta obra o partes de ella sean utilizadas para la realización de resúmenes de prensa.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra (www.conlicencia.com; 91 702 19 70 / 93 272 04 45).

Por tanto, este libro no podrá ser reproducido total o parcialmente, ni transmitirse por procedimientos electrónicos, mecánicos, magnéticos o por sistemas de almacenamiento y recuperación informáticos o cualquier otro medio, quedando prohibidos su préstamo, alquiler o cualquier otra forma de cesión de uso del ejemplar, sin el permiso previo, por escrito, del titular o titulares del copyright.

Thomson Reuters y el logotipo de Thomson Reuters son marcas de Thomson Reuters

Aranzadi es una marca de Thomson Reuters (Legal) Limited

© 2020 [Thomson Reuters (Legal) Limited / Miguel Rodríguez-Piñero Royo; Adrián Todolí Signes y otros]

© Portada: Thomson Reuters (Legal) Limited

Editorial Aranzadi, S.A.U.

Camino de Galar, 15

31190 Cizur Menor (Navarra)

ISBN: 978-84-1346-551-7

DL NA: 185-2020

Printed in Spain. Impreso en España

Fotocomposición: Editorial Aranzadi, S.A.U.

Impresión: Rodona Industria Gráfica, SL

Polígono Agustinos, Calle A, Nave D-11

31013 – Pamplona

Índice General

	<i>Página</i>
PRÓLOGO. LAS DOS ALMAS DEL DERECHO DEL TRABAJO DIGITAL	29
CAPÍTULO I	
EL IMPACTO DE LA DIGITALIZACIÓN SOBRE LOS DERECHOS FUNDAMENTALES LABORALES	35
JESÚS CRUZ VILLALÓN	
I. La irrupción transversal de la digitalización	36
II. La fortaleza de los derechos fundamentales como instrumento de tutela laboral	39
III. La tutela del trabajo autónomo como primer reto del proceso de digitalización	42
IV. Los derechos fundamentales del empleador como desafío en el espacio de la digitalización	47
V. Las incertidumbres del referente normativo en el ámbito territorial	54
VI. El espacio otorgado a la negociación colectiva en el marco de la digitalización	56
VII. La emergencia de la pujanza de nuevos derechos fundamentales: la protección de datos personales en la era de la digitalización	63

BLOQUE I: LA VIDEOVIGILANCIA

CAPÍTULO II

RÉGIMEN LEGAL DE LOS SISTEMAS DE CONTROL LABORAL BASADOS EN LA VIDEOVIGILANCIA: LAGUNAS Y ANTINOMIAS A LA LUZ DEL DERECHO COMUNITARIO	71
CRISTÓBAL MOLINA NAVARRETE	
I. Introducción: ¿logrado el “justo” equilibrio de derechos con una “razonable” seguridad jurídica?	72
II. Primera duda de disconformidad del art. 89 LOPD-GDD con el RGPD: lagunas en el juicio de justificación	75
III. De la licitud presunta de origen de la videocámara al límite de la transparencia de uso: laguna y antinomia	78
1. <i>Dos nuevas lagunas jurídicas para comenzar: el legislador “olvida” precisar que el deber de transparencia incorpora la finalidad del control</i>	<i>78</i>
1.1. Las deficiencias de regulación respecto de la dimensión individual de la garantía de transparencia del uso laboral de video-vigilancia	78
1.2. Ambigüedades de la faceta colectiva del deber de información: ¿Devaluar el contenido de la garantía a cambio de elevar su rango jurídico?	82
2. <i>Y una “antinomia” para cerrar el enfoque de gestión flexible: Condiciones de legitimidad de video-vigilancia “oculta” o “medio-oculta”</i>	<i>86</i>
2.1. Una norma de excepción pro eficacia de la prueba tecnológica: ¿la grabación de un “acto ilícito” subsana la ausencia de “información específica”?	86
2.2. La norma de excepción reafirmada por el TEDH: condiciones de legitimidad del uso del sistema de video-vigilancia encubierta u oculta	92
IV. Mayores límites a la “audiovigilancia”: solo al final comparece legalmente la proporcionalidad	96

	<i>Página</i>
V. Reflexión final: mejor ley específica, aun no propia, que nada, pero siempre que tenga calidad jurídica	98
VI. Bibliografía consultada	100

CAPÍTULO III

VIDEOVIGILANCIA Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LOS EMPLEADOS: UNA REVISIÓN DE LA DOCTRINA ADMINISTRATIVA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS	101
ANA BELÉN MUÑOZ RUIZ	

I. Introducción	102
II. La imagen y el sonido como dato personal	102
III. Las exigencias para la aplicación de la videovigilancia: legitimación, proporcionalidad, consentimiento e información	105
IV. Las garantías del régimen de protección de datos	114
1. <i>Las garantías de la calidad de los datos; en especial, la prohibición de usos incompatibles</i>	114
2. <i>Las obligaciones de secreto y seguridad, las limitaciones de la comunicación</i>	115
3. <i>Los derechos de las personas afectadas: acceso, rectificación, supresión y oposición</i>	116
V. Bibliografía	117

CAPÍTULO IV

ANÁLISIS DEL NUEVO RÉGIMEN JURÍDICO DEL DEBER DE INFORMACIÓN EN MATERIA DE VIDEOVIGILANCIA LABORAL ...	119
SEBASTIÁN HENRÍQUEZ TILLERÍA	
I. Planteamiento	120
II. Ámbito de aplicación y modalidades de cumplimiento del deber de información	122

	<i>Página</i>
III. Deber de información en la Ley Orgánica de Protección de Datos: ¿Un espejo de la doctrina del Tribunal Constitucional? ...	128
1. <i>Relación con la sentencia López Ribalda II, de 17 de octubre de 2019</i>	129
IV. Cuestionamientos a la coherencia de la Ley Orgánica de Protección de Datos Personales con el Reglamento General de Protección de Datos	131
V. El control oculto defensivo ex post: ¿Absoluto o relativo?	134
VI. Configuración legal del deber de información: un modelo de análisis en abstracto	136
VII. Conclusiones y propuestas	139
1. <i>Nuevo régimen impide el control por videovigilancia directo o primario de los trabajadores, legitimando únicamente el control indirecto o secundario</i>	139
2. <i>El control indirecto de la actividad laboral debe cumplir íntegramente el deber informativo del RGPD y con el derecho a información, consulta e informe de la representación de los trabajadores</i> ...	140
3. <i>Se prohíbe el control oculto absoluto, pero se legitima el control oculto relativo para el caso de comisión de actos ilícitos</i>	140
4. <i>Disconformidad normativa entre la LOPD y el Derecho de la Unión</i>	141
5. <i>Ventaja práctica del derecho a la protección de datos frente a otros derechos fundamentales</i>	141
5.1. <i>Propuestas de lege ferenda</i>	142
A. <i>Propuesta de “lege ferenda” N.º 1: modificar el art. 89.1 primer párrafo de la LOPD</i>	142
B. <i>Propuesta de “lege ferenda” N.º 2: modificar el art. 89.1 segundo párrafo de la LOPD</i>	142
VIII. Bibliografía	143

**BLOQUE II: LA GEOLOCALIZACIÓN, LOS WEREABLES
Y OTRAS FORMAS DE CONTROL**

CAPÍTULO V

	NUEVAS FORMAS DE CONTROL EMPRESARIAL: DESDE LOS GPS HASTA EL MÁS ALLÁ	147
	EVA MARÍA BLÁZQUEZ AGUDO	
I.	Introducción	148
II.	El derecho a la intimidad como límite natural de la utilización de los sistemas de geolocalización	150
	1. <i>Una somera revisión del juicio de ponderación como punto de salida</i>	151
	2. <i>La aplicación del juicio de ponderación al supuesto de la geolocalización</i>	154
III.	El límite del derecho a la protección de datos personales	156
	1. <i>La excepción al consentimiento</i>	157
	2. <i>La aplicación de los principios generales y la responsabilidad proactiva</i>	159
	3. <i>La información sobre los derechos de acceso, rectificación, limitación del tratamiento y supresión</i>	160
IV.	Elementos de uso de la geolocalización como control empresarial	161
	1. <i>La necesaria información de su utilización como medio de control</i>	162
	2. <i>La propiedad empresarial del instrumento de geolocalización durante la jornada de trabajo</i>	165
V.	Bibliografía	167

CAPÍTULO VI

ÚLTIMOS PERFILES DEL SISTEMA DE GEOLOCALIZACIÓN COMO INSTRUMENTO DEL EMPRESARIO	169
RAQUEL POQUET CATALÁ	
I. Introducción	170
II. El poder de control empresarial y las nuevas tecnologías de la información y la comunicación	171
III. El GPS como medio de control del trabajador	173
IV. Derecho a la intimidad del trabajador y derecho a la protección de datos	175
V. Respuestas de la doctrina constitucional y judicial	180
1. <i>Posición de la doctrina judicial europea</i>	180
2. <i>Posición del TC</i>	181
3. <i>Posición de la doctrina judicial</i>	183
VI. Conclusión	190
VII. Bibliografía	191

CAPÍTULO VII

RELACIÓN LABORAL DIGITALIZADA EN TÉRMINOS DE JUSTI- CIA Y CONTROL TECNOLÓGICO: ESPECIAL REFERENCIA AL SISTEMA DE GEOLOCALIZACIÓN	193
LUCÍA ARAGÜEZ VALENZUELA	
I. El control tecnológico de la prestación personal del trabajo	194
II. La invasión en la esfera privada de los trabajadores desde un enfoque de justicia social	197
III. Supuestos específicos de control: especial referencia al sistema de geolocalización	203
1. <i>Antes de la promulgación de la LOPDGDD</i>	208
2. <i>A posteriori de la LOPDGDD</i>	211

	<i>Página</i>
IV. Conclusiones	215
V. Anexo: bibliografía	216
CAPÍTULO VIII	
MONITORIZACIÓN: GPS, WEARABLES Y ESPECIAL REFERENCIA A LOS CONTROLES BIOMÉTRICOS PARA EL REGISTRO HORARIO. ASPECTOS PROCESALES	
CARLOS HUGO PRECIADO DOMÈNECH	
I. Introducción	219
II. GPS, wearables y controles biométricos en la nueva LOPD 3/2018, de 5 de diciembre	223
1. <i>Régimen jurídico de la geolocalización</i>	223
2. <i>Régimen jurídico de los wearables</i>	231
3. <i>Los datos biométricos y su utilización para el control horario</i>	234
III. Problemática procesal: la prueba electrónica y la ilicitud de la prueba	239
1. <i>Prueba electrónica</i>	239
1.1. <i>Cuestiones generales</i>	239
1.2. <i>Régimen jurídico</i>	243
A. <i>Régimen jurídico de la reproducción de palabra, sonido e imagen</i>	243
B. <i>Régimen jurídico de los instrumentos que permiten archivar y conocer datos relevantes para el proceso</i>	244
C. <i>Régimen jurídico en los supuestos de prueba inominada</i>	245
2. <i>Breve referencia a la problemática de la prueba ilícita</i>	247
2.1. <i>Origen y evolución de la doctrina la prueba ilícita ...</i>	247
A. <i>Concepto de prueba ilícita. Prueba ilícita vs. prueba ilegal</i>	251

	<i>Página</i>
2.2. Efectos de la prueba ilícita. La regla de exclusión y la doctrina de los frutos del árbol prohibido	254
A. La regla de exclusión	254
B. La doctrina de los frutos del árbol prohibido	258
C. Excepciones a la regla de exclusión	261
3. <i>Calificación del despido o de otras medidas laborales sustantivas derivadas de prueba ilícita</i>	263
IV. Bibliografía	269

BLOQUE III: BIOMETRÍA Y REGISTRO DE JORNADA

CAPÍTULO IX

REGISTRO DE JORNADA MEDIANTE CONTROLES BIOMÉTRICOS: UN CASO DE INCOHERENCIA EN EL DERECHO DEL TRABAJO DIGITAL	273
MIGUEL RODRÍGUEZ-PIÑERO ROYO	
I. Presentación: la inconsistencia fundacional del Derecho del Trabajo Digital	274
II. Delimitación de los “controles biométricos”	275
III. Los controles biométricos en las relaciones laborales	277
IV. Régimen jurídico de su utilización en las empresas	281
V. El uso de controles biométricos para el registro de jornada	286
1. <i>El deber de registrar la jornada de trabajo</i>	286
2. <i>Las dos visiones sobre el registro de jornada mediante controles biométricos</i>	292
VI. Conclusiones	298

	<u>Página</u>
CAPÍTULO X	
LÍMITES A LA BIOMETRÍA COMO MEDIO DE IDENTIFICACIÓN Y CONTROL DE LOS TRABAJADORES: NECESIDAD DE SU REGULACIÓN	301
FCO. JAVIER FERNÁNDEZ ORRICO	
I. Introducción	302
II. Datos biométricos: significado y concepto	303
III. Ventajas e inconvenientes de la biometría	305
IV. Sistemas biométricos	306
1. <i>Huella dactilar</i>	<i>306</i>
1.1. <i>Negativa del trabajador al control por medio de la huella digital.....</i>	<i>310</i>
2. <i>Iris</i>	<i>312</i>
V. Implantación del registro de jornada: su control por medios biométricos	313
1. <i>La nueva obligación legal de registro de jornada</i>	<i>314</i>
2. <i>Control de registro de jornada a través de sistemas de naturaleza biométrica</i>	<i>317</i>
VI. Límite al control biométrico	320
VII. Reflexiones, cuestiones y algunas respuestas	322
VIII. Bibliografía	325
CAPÍTULO XI	
EL REGISTRO DE LA JORNADA LABORAL Y LA PRIVACIDAD DE LOS TRABAJADORES	327
OLGA GARCÍA COCA	
I. Realidad normativa de la regulación del control horario	328
1. <i>Criterio técnico de la ITSS</i>	<i>330</i>
2. <i>Un acercamiento a la normativa europea acerca del registro de la jornada</i>	<i>332</i>

	<i>Página</i>
II. La digitalización de los distintos sistemas de control horario ...	335
III. Consecuencias del registro de datos de los trabajadores: ¿invasión de la intimidad versus control de la jornada?	340
1. <i>Pautas para el procesamiento de datos conforme a la LOPDGDD</i>	342
2. <i>Desconexión digital y control horario</i>	348
IV. Algunas consideraciones finales	349
V. Bibliografía	351

BLOQUE IV: REGISTRO ORDENADORES

CAPÍTULO XII

ACCESO A DISPOSITIVOS DIGITALES DEL TRABAJADOR FACILITADOS POR LA EMPRESA	355
--	-----

MANUEL LUQUE PARRA
FRANCISCO RAMÓN LACOMBA

I. Introducción	357
II. Contextualización	361
1. <i>Delimitación del objeto del acceso</i>	362
1.1. <i>Cuando hablamos de acceso al ordenador, ¿hablamos solo del acceso al e-mail?</i>	362
1.2. <i>Entonces, ¿la facultad de acceso y control por la empresa se ha de sujetar a los mismos límites cuando se trate de smartphones o iphones, una tablet, un USB o cualquier otro recurso electrónico o telemático que facilite la empresa?</i>	362
1.3. <i>Qué sucede con los emails que envía el trabajador desde la dirección profesional, pero accediendo desde su ordenador personal</i>	362
2. <i>Delimitación del objetivo del acceso</i>	362
2.1. <i>¿Cuáles son las finalidades legítimas del control y acceso a dispositivos digitales que activarían el riesgo sobre los derechos fundamentales del trabajador?</i>	362

	<i>Página</i>
2.2. ¿Cuál podría ser un ejemplo de acceso a ordenadores con finalidad preventiva?	363
2.3. ¿Cuál podría ser un ejemplo de acceso a ordenadores con finalidad reactiva?	363
2.4. ¿Existe alguna finalidad preventiva del acceso a ordenadores que la empresa pueda verse obligada a atender por exigencia legal?	364
2.5. ¿Cuál podría ser un ejemplo de acceso a ordenadores con la finalidad de comprobar la desconexión digital del trabajador?	364
3. <i>Delimitación del debate procesal</i>	366
3.1. ¿Qué significa doctrina de los frutos del árbol envenenado?	366
3.2. ¿Existe una posición mayoritaria respecto a que la ilicitud de la prueba del acceso a ordenadores conlleve la nulidad de la medida empresarial?	367
III. Dimensión constitucional: sus parámetros de licitud	373
1. <i>¿Qué derechos fundamentales están en juego?</i>	374
2. <i>Los derechos fundamentales afectados por el acceso al ordenador ¿son un límite infranqueable que impide cualquier acceso?</i>	374
3. <i>Las facultades de vigilancia y control que confiere el art. 20.3 ET ¿permiten entonces a la empresa un examen ilimitado de sus dispositivos digitales puestos a disposición de los trabajadores?</i>	375
4. <i>¿Podría la empresa, como alternativa, eliminar la presencia de tales derechos fundamentales en la empresa prohibiendo completamente el uso privado de los ordenadores y otros dispositivos digitales?</i>	375
5. <i>¿Cuándo incurrirá la empresa en una intromisión ilegítima en los derechos fundamentales del trabajador al registrar su ordenador u otro dispositivo digital facilitado para su trabajo?</i>	376
6. <i>¿Es suficiente para determinar la licitud del acceso empresarial a los dispositivos digitales la aplicación estricta del indicado principio de proporcionalidad?</i>	376

	<i>Página</i>
IV. Los parámetros legales de licitud	378
1. <i>¿Existe una previsión específica en la LOPDGDD en materia de acceso a ordenadores y otros dispositivos digitales?</i>	378
2. <i>¿Qué alcance debe atribuirse a tan trascendental reconocimiento expreso del derecho a la intimidad de los trabajadores en el uso de los dispositivos digitales en el ámbito laboral?</i>	379
3. <i>¿Cuáles son las pautas de actuación empresarial que establece el art. 87 LOPDGDD para que el acceso a los dispositivos digitales sea válido?</i>	380
4. <i>¿Serían válidas las cláusulas contractuales firmadas por el trabajador en su contrato en cuya virtud autorizase a la empresa a la instalación de aplicaciones que permitiesen el acceso a la actividad del ordenador?</i>	381
5. <i>¿Quedaría legitimada la empresa, mediante el citado art. 87 LOPDGDD, para reutilizar la información obtenida mediante el acceso/monitorización de los dispositivos digitales que utiliza el trabajador?</i>	381
6. <i>¿Sería válida la prueba obtenida unilateralmente mediante el acceso a dispositivos digitales en la empresa que no disponga de criterios de utilización?</i>	382
7. <i>¿A qué se refiere el art. 87.3 LOPDGDD cuando requiere que, en la elaboración de los criterios de utilización de los dispositivos digitales, deberán “participar” los representantes de los trabajadores?</i> ...	382
8. <i>¿Sería válida la prueba obtenida aun disponiendo de criterios de uso de dispositivos digitales, pero en cuya elaboración no haya participado la representación legal de los trabajadores (RLT) o lo haya hecho sin respetar la empresa las exigencias de la buena fe (por ejemplo, sin facilitarles información suficiente para emitir opinión/informe)?</i>	383
9. <i>¿Qué sucede si no existen en la empresa representantes legales de los trabajadores a los que hacer participar para la elaboración de los criterios de utilización de dispositivos digitales?</i>	383
10. <i>¿Qué sucede si existe representación legal de los trabajadores en unos centros de trabajo y en otros no?</i>	383

	<u>Página</u>
11. ¿Sería válida la prueba obtenida mediante el acceso a dispositivos digitales sin haber informado previa y suficientemente a los trabajadores acerca de sus reglas de uso?	384
V. Evolución judicial en relación con los parámetros de licitud del acceso a los dispositivos digitales	384
1. <i>Etapa pre-Bărbulescu II</i>	384
1.1. ¿Cuál era la posición de los tribunales antes de Bărbulescu-II?	384
1.2. ¿Se han encontrado siempre alineadas la jurisdicción social y penal en esta materia?	386
2. <i>STEDH 05-09-2017 (Bărbulescu II)</i>	387
2.1. ¿Cuáles son los antecedentes de hecho de esta importante Sentencia?	387
2.2. ¿En qué sentido se pronunció el TEDH en su primera Sentencia, Bărbulescu I?	388
2.3. ¿Cuál es el criterio que, finalmente, aplica el TEDH en su segunda Sentencia, Bărbulescu-II?	389
3. <i>Etapa post Bărbulescu-II</i>	392
3.1. ¿Se está recibiendo la doctrina Bărbulescu-II en las Sentencias dictadas con posterioridad?	392
3.2. Tras Bărbulescu II y la LOPDGDD, ¿qué deberían señalar los Tribunales en relación con los códigos de tolerancia cero en relación con el uso privado de los dispositivos digitales facilitados por la empresa?	393
3.3. Tras Bărbulescu II y la LOPDGDD, ¿qué contenido han de tener los “criterios de utilización” de los dispositivos digitales facilitados por la empresa a los trabajadores?	393
3.4. Tras Bărbulescu II, ¿otorgaría el art. 87 LOPDGDD base de legitimación para el acceso al ordenador basado en meras sospechas?	394
3.5. Tras Bărbulescu II y la LOPDGDD, si la empresa respeta –en su acceso al dispositivo digital– las “reglas del juego” (criterios de uso fijados y comunicados internamente) ¿el acceso sería ya per se válido?	395

	<i>Página</i>
VI. Pautas de gestión empresarial	396
1. <i>A la vista de la LOPDGDD y de la doctrina judicial europea, ¿cuáles serían las pautas de gestión empresarial claramente establecidas?</i>	396
2. <i>En nuestra opinión, ¿cuáles serían otras 6 pautas adicionales de gestión empresarial que consideramos que deberían tenerse también en cuenta por las empresas?</i>	397
VII. Conclusiones	398
VIII. Bibliografía	398
CAPÍTULO XIII	
LA PROTECCIÓN DE DATOS DE LOS TRABAJADORES EN PORTUGAL: EL DIÁLOGO ENTRE EL CÓDIGO DE TRABAJO, EL RGPD Y LA NUEVA LEY DE PROTECCIÓN DE DATOS	
	401
ANA LAMBELHO	
MARISA DINIS	
I. Consideraciones iniciales	401
II. La protección de datos personales de los trabajadores en el Código de Trabajo	404
III. La protección de datos personales de los trabajadores en el RGPD	407
IV. La nueva Ley de Protección de Datos portuguesa y la protección de datos personales de los trabajadores	410
V. Consideraciones sobre el diálogo, necesario y posible, entre el Código de Trabajo, el RGPD y la nueva Ley de Protección de Datos	413
VI. Bibliografía	419

BLOQUE V: LA REPUTACIÓN DIGITAL DE LOS TRABAJADORES COMO FORMA DE CONTROL

CAPÍTULO XIV

REPUTACIÓN DIGITAL Y EFECTOS SOBRE LOS TRABAJADORES: REDES SOCIALES PARA CONTRATACIÓN, USOS Y LÍMITES	425
FRANCISCO JAVIER CALVO GALLEGO	

I. Introducción: la tutela de la personalidad del trabajador en los procesos de selección. Algunas notas	427
II. La reputación digital del trabajador: razones de su aparición y de su importancia. El papel de las redes sociales	441
1. <i>Un primer intento de aproximación al concepto de reputación laboral</i>	442
2. <i>La reputación laboral y sus implicaciones</i>	446
3. <i>La progresiva importancia de la reputación y su naturaleza paulatinamente digital: mercados transicionales, trabajo en plataformas y expansión de la “transparencia” en la sociedad de la información</i>	452
III. Reputación digital externa o en la red y reputación digital interna en la empresa y en la plataforma: algunos problemas y límites ...	459
1. <i>Reputación digital y datos personales en las redes sociales</i>	460
2. <i>Reputación interna y sistemas de valoración</i>	467

CAPÍTULO XV

LA EVALUACIÓN DE LOS TRABAJADORES POR PARTE DE LOS CLIENTES (LA LLAMADA “REPUTACIÓN DIGITAL”) Y LA PREVENCIÓN DE RIESGOS LABORALES	473
ADRIÁN TODOLÍ SIGNES	

I. La evaluación de los trabajadores por parte de los clientes	473
1. <i>Concepto y tipos de sistemas de reputación digital de trabajadores</i>	473
2. <i>El incremento del poder de los clientes para tomar decisiones jurídicas sobre los trabajadores</i>	476

	<i>Página</i>
II. Factores de riesgo laboral derivados del uso de un sistema de sistemas de reputación digital para monitorizar el trabajo	477
III. Posibles perjuicios para la salud de los trabajadores sujetos a un sistema de reputación digital	480
IV. Medidas para reducir los riesgos para la salud de los trabajadores sometidos a un sistema de reputación digital	482
1. <i>Evaluación de los riesgos concretos</i>	482
2. <i>Cursos de sensibilización</i>	483
3. <i>Transparencia en la razón de la evaluación</i>	483
4. <i>Posibilidad de réplica para el trabajador</i>	483
5. <i>Más de una pregunta</i>	484
6. <i>No publicar las evaluaciones</i>	484
V. Bibliografía	485
CAPÍTULO XVI	
LA REPUTACIÓN DIGITAL MEDIANTE ALGORITMOS Y LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES	
ALEXANDRE PAZOS PÉREZ	
I. Introducción	488
II. Los sistemas reputacionales en las plataformas digitales	490
III. Los algoritmos y los derechos fundamentales de los trabajadores	493
IV. El derecho a la protección de datos y el derecho a la desconexión en la era digital	494
V. Conclusiones	497
VI. Bibliografía	502

	<i>Página</i>
CAPÍTULO XVII	
TRABAJO, ALGORITMOS Y DISCRIMINACIÓN	505
ANTONIO FERNÁNDEZ GARCÍA	
I. Los algoritmos en la relación laboral	506
II. Los algoritmos y la discriminación	511
III. La discriminación en el trabajo	515
1. <i>La discriminación directa</i>	516
2. <i>La discriminación indirecta</i>	517
3. <i>La discriminación múltiple</i>	518
4. <i>La discriminación por asociación</i>	520
5. <i>La discriminación por error</i>	523
IV. ¿Es la discriminación algorítmica una nueva tipología de discriminación?	524
V. Conclusiones	527
VI. Bibliografía	528

**BLOQUE VI: PREVENCIÓN DE RIESGOS LABORALES Y
CONTROL DIGITAL**

CAPÍTULO XVIII	
SISTEMAS DE PREVENCIÓN Y PROTECCIÓN EN EL ORDEN SOCIAL SOBRE LOS RIESGOS EMERGENTES DE ORIGEN PSICO-SOCIAL EN LA ECONOMÍA DIGITAL	535
RAÚL PAYÁ CASTIBLANQUE RICARD CALVO PALOMARES	
I. Introducción	536
II. Metodología	539
1. <i>Análisis estadístico</i>	539
1.1. Fuentes	539

	<i>Página</i>
1.2. Variable dependiente	539
1.3. Variables independientes	540
1.4. Covariables	542
1.5. Análisis estadístico	543
2. <i>Análisis del discurso</i>	544
III. Resultados	545
1. <i>Análisis estadístico</i>	545
1.1. Condiciones de empleo del Trabajo Digital	545
1.2. Exposición a factores de riesgo laboral de los/as trabajadores/as digitales	547
1.3. Consecuencia para la salud del trabajo digital y contingencias profesionales	549
2. <i>Análisis jurídico y del discurso</i>	551
2.1. Niveles de prevención de los riesgos psicosociales que afectan al trabajo digital	551
2.2. Niveles de protección en el sistema de protección social de las patologías referidas en el trabajo digital	562
IV. Discusión y conclusiones	567
V. Bibliografía	571

CAPÍTULO XIX

EL SISTEMA DE PREVENCIÓN DE RIESGOS LABORALES COMO GARANTÍA DE EFECTIVIDAD DEL DERECHO A LA DESCONEXIÓN DIGITAL	577
--	------------

MARGARITA MIÑARRO YANINI

I. Introducción: las débiles fronteras entre lo laboral y lo extralaboral y su impacto en la salud	577
II. La nueva regulación de la LOPDGDD: un análisis desde el punto de vista preventivo	580

	<i>Página</i>
1. <i>Nuevos riesgos derivados de la hiperconectividad: la fatiga digital</i>	580
2. <i>Medidas de prevención: la desconexión digital fuera del trabajo</i>	583
III. La desconexión digital en la negociación colectiva y su escaso tratamiento desde la dimensión de la prevención de riesgos laborales	586
1. <i>La importancia de la negociación colectiva en la configuración y efectividad del derecho a la desconexión digital</i>	586
2. <i>La negociación colectiva relativa a la desconexión digital</i>	587
2.1. Dimensión de conciliación	587
A. Instrumentos en materia de igualdad	587
B. Convenios colectivos y acuerdos de empresa	588
2.2. Dimensión preventiva	590
A. Regulación convencional de ámbito de empresa ...	590
B. Marco autonómico	592
IV. Conclusiones	593
V. Bibliografía	594

CAPÍTULO XX

LA NECESARIA EVALUACIÓN DE RIESGOS Y ADOPCIÓN DE MEDIDAS PREVENTIVAS PARA UNA CORRECTA POLÍTICA EMPRESARIAL Y EFICACIA REAL DE LA DESCONEXIÓN DIGITAL	597
--	------------

JOSÉ M^a QUÍLEZ MORENO

I. Del interés por el trabajo decente	598
II. Del estrés laboral causado por las nuevas tecnologías	600
III. De las medidas legislativas acerca de la desconexión digital	603
IV. De las medidas prácticas a aplicar para conseguir una efectiva desconexión digital	606
V. Bibliografía	609

CAPÍTULO XXI

DIGITALIZACIÓN, MONITORIZACIÓN Y PROTECCIÓN DE LA SALUD: MÁS ALLÁ DE LA “FATIGA” INFORMÁTICA	613
MARÍA TERESA IGARTUA MIRÓ	
I. El punto de partida	614
II. Algunos efectos de la llamada “digitalización”: invasión de espacios personales e incremento de la monitorización	616
III. Nuevos riesgos laborales	620
1. <i>La tecno-invasión: riesgos para la seguridad y salud</i>	620
2. <i>El estrés laboral o la epidemia del siglo XXI</i>	623
IV. La tutela integral de la salud: más allá de la fatiga informática ...	627
1. <i>Plasmación legal de la evitación de la fatiga informática</i>	627
2. <i>La tutela integral de la salud</i>	629
V. Desarrollo tecnológico, cambios en la organización del trabajo y prevención	631
1. <i>Desarrollo tecnológico y obligación de seguridad</i>	631
2. <i>Cambios tecnológicos, organización del trabajo y persona del trabajador</i>	634
VI. Prevención integrada y renovado valor de los principios preventivos	636
1. <i>Hacia la definitiva integración de la prevención en la empresa ...</i>	636
2. <i>Un renovado valor de los principios de la acción preventiva</i>	637
3. <i>¿Del principio de prevención al de precaución?</i>	638
VII. A modo de epílogo: el “bienestar organizativo” como meta	641
VIII. Bibliografía citada	643

CAPÍTULO XXII

ACOSO EN EL TRABAJO POR MEDIO DE DISPOSITIVOS DIGITALES Y SU REPERCUSIÓN EN LA SALUD DE LA PERSONA TRABAJADORA: ¿NO ES MOMENTO DE TOMARNOS EN SERIO SU PREVENCIÓN?	649
FERNANDO DE VICENTE PACHÉS	
I. Preliminar. La necesaria y justificada prevención del acoso laboral por medio de dispositivos digitales	650
II. Una aproximación al acoso laboral a través de dispositivos digitales ¿un nuevo fenómeno de violencia en el trabajo?	652
III. La repercusión del acoso digital en la salud de las personas trabajadoras	655
IV. Configuración del acoso digital en el trabajo	658
V. Supuestos frecuentes de acoso digital laboral	661
1. <i>Distribuir en internet imágenes o datos delicados</i>	661
2. <i>Ridiculizar o estigmatizar en espacios web</i>	663
3. <i>Usurpar la identidad de la víctima y –en su nombre y desde el anonimato– realizar comentarios ofensivos</i>	663
4. <i>Acceder al ordenador de la víctima</i>	664
5. <i>Realizar en redes sociales comentarios ofensivos, opiniones y declaraciones insultantes o amenazantes</i>	665
6. <i>Acciones de presión para actuar conforme a las solicitudes del acosador digital</i>	668
7. <i>Uso del teléfono móvil como instrumento de acoso digital</i>	669
VI. La protección del acoso digital desde la normativa preventiva	670
VII. Bibliografía de referencia	676

Thomson Reuters ProView. Guía de uso