REVISTA ELECTRÓNICA
DE ACCESO ABIERTO
ISSN 2282-2313

Revista Internacional y Comparada de

RELACIONES LABORALES Y DERECHO DEL EMPLEO

ADAPT
www.adapt.it
UNIVERSITY PRESS

Revista Internacional y Comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO

Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT

El uso de la inteligencia artificial en la prevención de riesgos laborales*

María del Carmen AGUILAR DEL CASTILLO**

RESUMEN: La capacidad de control que permite el uso de la inteligencia artificial (IA) y la *Internet of Things* (IoT), a través de la obtención de datos y su tratamiento algorítmico, facilitan determinar el alcance de la obligación de seguridad del empresario como garante de la salud de sus trabajadores y la conducta del trabajador como elemento exonerante o atenuante de la responsabilidad del empresario. La posibilidad de identificar situaciones potenciales de riesgo o conductas indebidas de los trabajadores, entre otras, por la automatización de tareas o por una habituación del riesgo hace que se puedan dar las órdenes e instrucciones necesarias para evitar las situaciones de riesgo. Su incumplimiento constituye una infracción de las obligaciones básicas del trabajador alejándose con ello de una posible conducta no temeraria. El tratamiento de los datos con una finalidad preventiva implica un mayor control de los riesgos lo que debe conllevar una mayor protección y una disminución de situaciones peligrosas lo que implicaría por parte del trabajador un mayor grado de intencionalidad en conductas de riesgo y, por otro lado, una disminución del deber objetivo de cuidado del empresario.

Palabras clave: Obligación de seguridad, imprudencia, inteligencia artificial, Internet of Things, algoritmos, vigilancia y control.

SUMARIO: 1. Introducción. 2. La conducta del trabajador y la responsabilidad penal del empresario. 3. Elementos de la imprudencia. 4. La IA, la IoT y el poder del empresario. 5. Información "inteligente" al servicio de la prevención. 5.1. La prevención de los riesgos laborales como contenido de la IA. 5.2. La prevención de los riesgos, el tratamiento de los datos y el nivel de complejidad de la IA. 6. Los datos como fuente de información de la evaluación de riesgos. 7. La información como requisito en la obtención de datos. 8. El "riesgo permitido", la conducta del trabajador y la IA. 9. La IA y la IoT: herramientas al servicio del empresario. 10. Conclusiones. 11. Bibliografía.

* Este trabajo se enmarca en el proyecto de investigación Plan Estatal 2017-20, Retos investigación, *Nuevas dinámicas y riesgos sociales en el mercado de trabajo del siglo XXI: desigualdad, precariedad y exclusión social*, RTI2018-098794-B-C31.

** Profesora colaboradora doctora, Universidad de Sevilla (España).

The Use of Artificial Intelligence in the Prevention of Work Risks

ABSTRACT: The control capacity that allows the use of Artificial Intelligence (AI) and Internet of Things (IoT), through obtaining data and their algorithmic treatment, facilitates determining the scope of entrepreneurs' safety obligation as guarantor of the health of their workers, and the workers' behaviours as an exempting or attenuating element of entrepreneurs' responsibilities. The possibility of identifying potential risk situations or the workers' misconduct, among other matters, by the automatization of tasks or by a familiarity of the risk means that the necessary orders and instructions can be given to avoid risk situations. Their non-compliance is an infringement of the worker's basic obligations, non-reckless behaviour thus becoming less likely. The data treatment with a preventive purpose involves a greater control of risks. This leads to more protection and a decrease in dangerous situations, implying a greater degree of the workers' intent in risk behaviours and, on the other hand, a decrease of the entrepreneurs' objective duties of care.

Key Words: Safety obligation, imprudence, Artificial Intelligence, Internet of Things, algorithms, surveillance and control.

1. Introducción

La naturaleza jurídica de la prevención de riesgos laborales hace que la relación de subordinación como elemento identitario de la relación laboral nos lleve a situar al empresario en una posición de garante de la seguridad de los trabajadores. Es esta posición la que define el conjunto de derechos y obligaciones de trabajadores y empresario.

La obligación general del empresario de proteger eficazmente la salud del trabajador adoptando cuantas medidas sean necesarias se encuentra en relación con el deber de cumplimiento y cooperación del trabajador con su empresario. Relación que necesariamente ha de desarrollarse bajo el cumplimiento de la norma y de los principios preventivos previstos en el art. 15 de la Ley de prevención de Riesgos Laborales (LPRL)[1].

De entre los distintos principios de la acción preventiva, es obligación del empresario prever las imprudencias no temerarias del trabajador. Es el único principio que puede llegar a tener connotaciones negativas por cuanto, incluso ante un incumplimiento del empresario, su posición de garante puede quedar diluida ante una determinada conducta del trabajador. La confusa dicción de este principio puede hacer recaer sobre el concepto de imprudencia, término nada pacífico entre la doctrina y la jurisprudencia, el establecimiento de la frontera del "riesgo permitido" y, en consecuencia, el alcance de la posición deudora del empresario frente al trabajador.

Las nuevas tecnologías como medios intrínsecos a la propia organización de la empresa pueden, constituirse como "herramientas" adecuadas para, desde la obtención de datos y su manipulación, identificar y prevenir los riesgos relacionados con la conducta del trabajador. Estas nuevas tecnologías pueden llegar a tener un efecto clarificador sobre el concepto de la imprudencia no temeraria, toda vez que dentro de la relación laboral solo se entiende en oposición a la obligación del empresario de proteger eficazmente la salud de sus trabajadores. Su utilización en la identificación del riesgo puede llegar a redefinir el concepto de imprudencia no temeraria a través del control de su previsibilidad.

Entre las consecuencias que la irrupción de las nuevas tecnologías está produciendo en las empresas a través de su digitalización, robotización, el uso de la *Internet of Things* (IoT)[2] o la inteligencia artificial (IA), entre otras,

[1] Ley 31/1995, de 8 de noviembre (en *BOE*, 10 noviembre 1995).

[2] «Se dice que nació para mejorar la competitividad de cualquier institución […] de manera intersectorial, apostando por una vida mejor, a través de dispositivos interconectados que sean capaces de obtener "indicadores métricos de uso y, en función de eso, ejecutar acciones diseñadas por sus programadores […]"» (S. BARONA VILAR,

se está dando una alteración de las relaciones laborales tal y como las conocemos, produciéndose, cada vez con más frecuencia, un desvanecimiento de esta relación como una actividad desarrollada dentro del ámbito de organización y dirección de otra persona.

Actualmente nos podemos encontrar empresas tradicionales con un sistema de trabajo también tradicional frente a otras que, realizando la misma actividad, han ido modernizándose e introduciendo nuevas tecnologías que han ido desplazando a la mano de obra. La convivencia de puestos de trabajo y/o actividades que, en un futuro más o menos lejano provocará la eliminación de puestos de trabajo e incluso de la propia actividad, genera, sobre todo, incertidumbre sobre la capacidad de respuesta de nuestra sociedad.

La velocidad como seña de identidad de la tecnología parece estar provocando una subordinación general de la sociedad. No se trata, sin embargo, de establecer una disección entre bueno o malo, ético o no; simplemente es una realidad a la que hay que adaptarse para que las nuevas tecnologías sigan estando a nuestro servicio y no a la inversa.

El objeto de este trabajo no es cuestionar la evolución, pero sí reflexionar sobre la posición de los empresarios ante estas nuevas realidades y sobre el contenido de su obligación como garante de la salud de los trabajadores con independencia de la actividad que éstos desarrollen o puesto de trabajo que ocupen.

2. La conducta del trabajador y la responsabilidad penal del empresario

Todo daño resultante de un accidente de trabajo puede deberse a un incumplimiento del deber de seguridad del empresario, a unas conductas inseguras o descuidadas del trabajador, a una conjunción de ambas o simplemente a la mala suerte[3]. Cuando se produce el elemento dañoso la pregunta principal que hay que formular es ¿quién es el responsable? Y es aquí donde la interpretación y aplicación de la norma ha de ser clara y precisa, debiendo tenerse en cuenta, las características de la relación laboral, la posición de los sujetos dentro de la misma y las obligaciones jurídico-preventivas de cada uno de ellos.

Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?, en *Revista Boliviana de Derecho*, 2019, n. 28, p. 30).

[3] M. COBO DEL ROSAL, J. SANCHEZ-VERA GÓMEZ-TRELLEZ, *Responsabilidad penal por accidentes laborales*, en *Cuadernos de Política Criminal*, 2004, n. 82.

Como ya se ha señalado la LPRL y el Estatuto de los Trabajadores[4] definen como sujeto obligado al empresario, pudiendo dar lugar sus incumplimientos en la materia a distintas responsabilidades, entre ellas la responsabilidad penal. Aunque no es la única, la conducta del trabajador puede dar lugar a una exoneración de culpa del empresario[5].

La atribución de la titularidad subjetiva del delito no solo va a venir condicionada por la norma sino por la interpretación que se haga de ella. La necesidad de establecer la frontera del "riesgo permitido", para a partir de ella prever los mecanismos necesarios para hacerla respetar, contrasta con las características que define al delito contra la seguridad de los trabajadores (arts. 316-318 del Código Penal (CP)). Su carácter de norma penal en blanco[6] hace que tengamos que acudir a otros ordenamientos jurídicos como el laboral para definir la conducta delictiva, que en todo caso recae sobre el sujeto obligado.

Por definición el empresario, como garante de la seguridad de sus trabajadores, es el sujeto obligado, aunque penalmente pueda no ser el responsable[7]. El incumplimiento de la normativa preventiva, generando un riesgo grave para los trabajadores, conlleva *per se* la transgresión de la frontera de una conducta penalmente permitida. No obstante, la participación en la misma de una conducta "inapropiada" o "descuidada" del trabajador puede convertir en irrelevante esta transgresión.

Es, por tanto, la conducta del trabajador y el grado de exigibilidad en el cumplimiento de sus obligaciones por parte del empresario lo que, desde un punto de vista penal, podrá tener trascendencia en la existencia de una conducta punible para este.

Respecto de la conducta del trabajador, la imprudencia "no temeraria", por continuar con la terminología legal, es una manifestación del concepto de imprudencia que se aleja de sus connotaciones penales, pero que ha de participar de su esencia y de sus elementos para determinar la irrelevancia de la conducta del trabajador frente a la posible comisión de un delito por parte del empresario.

Los arts. 316-319 ss. CP[8] ubicados dentro del capítulo «de los delitos

[4] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en *BOE*, 24 octubre 2015).

[5] A. MONGE FERNÁNDEZ, *Aspectos básicos sobre responsabilidad penal por riesgos en la construcción*, en A. MONGE FERNÁNDEZ (dir.), *Responsabilidad y construcción. Aspectos fundamentales*, Tirant lo Blanch, 2017, pp. 438-440.

[6] *Ibidem*, pp. 417-420.

[7] M.T. IGARTUA MIRÓ, *Sistema de prevención de riesgos laborales*, Tecnos, 2018, pp. 404-405.

[8] Art. 316 CP: «Los que con infracción de las normas de prevención de riesgos laborales y estando legalmente obligados, no faciliten los medios necesarios para que los trabajadores desempeñen su actividad con las medidas de seguridad e higiene adecuadas,

contra los derechos de los trabajadores», forman parte de los denominados delitos de riesgo en los que la conducta tipificada consiste en generar un riesgo grave a la vida, salud e integridad física de los trabajadores, por no facilitar los medios necesarios para que puedan desarrollar su actividad con seguridad, por quienes esté obligados a ello. La falta de un resultado lesivo para la realización de este tipo penal hace que la imprudencia del trabajador solo pueda tener relevancia en la medida en la que el riesgo existente provoque un resultado dañoso y es aquí cuando la calificación de su conducta como imprudente será determinante para exonerar o atenuar la responsabilidad penal del sujeto obligado que coincide con el empresario o persona en quien este delegue[9].

Es a partir de la conceptuación de la imprudencia cuando se ha de valorar la aplicación y el respeto del principio preventivo previsto en el art. 15.4 LPRL, sobre la obligación del empresario de prever las imprudencias no temerarias del trabajador. Se trata de identificar los elementos de la imprudencia punible en la conducta del trabajador, no para convertirlo en el reo del delito en la medida en la que, la autolesión no es punible, sino para exonerar de responsabilidad penal a quién sí la tiene si se produce este resultado.

La LPRL es una ley de carácter preventivo por lo que todo su contenido tiene por objeto prevenir los riesgos derivados del trabajo[10] dando lugar su incumplimiento a una posible responsabilidad penal del sujeto obligado[11], recogida de forma expresa en el art. 316 CP. No obstante el carácter de la norma, no puede ignorarse la posibilidad de que se produzca un daño[12] como consecuencia de la existencia de un riesgo grave, lo que extiende la responsabilidad penal no solo a un tipo, como es el previsto en el art. 316, sino también puede dar lugar a la comisión de otros delitos, en concurso, como el de homicidio[13] o lesiones[14] generalmente de carácter imprudente y es, en estos casos, cuando la conducta del trabajador adquiere una gran

---

de forma que pongan así en peligro grave su vida, salud o integridad física, serán castigados con las penas de prisión de seis meses a tres años y multa de seis a doce meses».

[9] A. MONGE FERNÁNDEZ, *op. cit.*, pp. 461-465.

[10] Art. 2.1 LPRL.

[11] Art. 42.1 LPRL: «El incumplimiento por los empresarios de sus obligaciones en materia de prevención de riesgos laborales dará lugar a responsabilidades administrativas, así como, en su caso, a responsabilidades penales».

[12] Art. 4.3 LPRL: «Se considerarán como "daños derivados del trabajo" las enfermedades, patologías o lesiones sufridas con motivo u ocasión del trabajo».

[13] Art. 142 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en *BOE*, 24 noviembre 1995).

[14] Art. 152 CP.

transcendencia.

3. Elementos de la imprudencia

Sin entrar en las distintas discusiones doctrinales sobre el concepto de imprudencia, lo que nos interesa es definir, aunque sea brevemente, los distintos elementos que la configuran. Solo desde su análisis podríamos entender cuando la conducta del trabajador es relevante frente a la conducta previa del empresario en el cumplimiento de su obligación como garante de la seguridad.

Una de las primeras características de la imprudencia es su causalidad, por lo que solo tras el enjuiciamiento de la conducta imprudente podemos determinar su relevancia penal. En el delito contra la seguridad de los trabajadores será la falta de los elementos propios de la imprudencia en la conducta del trabajador la que atenúe o exima de responsabilidad al empresario.

En la relación laboral la protección de la salud de los trabajadores, a través de la adopción y cumplimiento de cuantas medidas sean necesarias, ha de ser la primera consideración a tener en cuenta cuando nos enfrentamos ante una posible imprudencia del trabajador, ya que esta conducta si tendrá relevancia cuando el empresario cumpla adecuadamente con su deber objetivo de cuidado, con la formación preventiva, la adopción de los medios necesarios y la necesaria vigilancia del cumplimiento por parte del trabajador de sus obligaciones[15].

Principios como el de autorresponsabilidad y consentimiento de la víctima difícilmente encuentran encaje dentro de la relación laboral por la posición que el trabajador ocupa en la misma. La exigencia de capacidad para autoorganizarse como requisito de la autorresponsabilidad desaparece en la relación laboral en la medida en la que el trabajador no tiene libertad para desarrollar su actividad y no reúne «las condiciones esenciales de conocimiento y voluntad para autoorganizarse»[16].

La ajeneidad y la dependencia o subordinación como requisitos esenciales de la prestación de trabajo dificultan considerablemente la participación del trabajador en la organización y sistema de gestión de la empresa impidiendo su autoorganización[17]. Pero, también «niegan la validez del

[15] Arts. 29 LPRL y 5.b del texto refundido del Estatuto de los Trabajadores (TRET).

[16] J.A. LASCURAÍN SÁNCHEZ, *La prevención penal de los riesgos laborales: cinco preguntas*, en AA.VV. (coords.), *Estudios penales en homenaje al profesor Cobo del Rosal*, Dykinson, 2005, pp. 566 y 586-591.

[17] Art. 20.1 TRET.

consentimiento como causa de justificación»[18]. Por un lado, porque el trabajador no dispone de toda la información sobre el ciclo completo de producción ni conoce todos los riesgos que del mismo se derivan y, por otro, porque la propia legislación laboral lo impide. La LPRL establece que el trabajador tiene derecho a una protección eficaz de su salud, derecho básico del trabajador al que no puede renunciar[19] y que incluye, entre otras, la obligación del empresario de adoptar cuantas medidas sea necesarias para evitar los riesgos. Reforzando esta posición deudora con la obligación de prever las imprudencias no temerarias del trabajador, la propia Ley de la Jurisdicción Social (LJS)[20] señala que «No podrá apreciarse como elemento exonerador de la responsabilidad la culpa no temeraria del trabajador ni la que responda al ejercicio habitual del trabajo o a la confianza que éste inspira»[21].

La interpretación de la norma desde la perspectiva que estamos adoptando no coincide plenamente con la que, en ocasiones, hacen nuestros tribunales exonerando al empresario de responsabilidad, aunque no haya cumplido con su obligación de seguridad por entender que el trabajador ha asumido un riesgo que no le correspondía y que podía y debía haber evitado[22]. En otras ocasiones reduce esta responsabilidad al

[18] J.A. LASCURAÍN SÁNCHEZ, *op. cit.*, pp. 566 y 586-591.

[19] Art. 3 TRET.

[20] Ley 36/2011, de 10 de octubre (en *BOE*, 11 octubre 2011).

[21] Art. 96.2 LJS. En este ámbito resulta contundente los pronunciamientos de las Sentencias del Tribunal Supremo de 26 de marzo de 1999, 11 de diciembre de 2002 y 18 de enero de 1995. En contra de esta afirmación la Audiencia Provincial de Barcelona (Sección 2ª), sentencia n. 665/2003 de 2 de septiembre, FJ 3 (ARP 2003/619). Considera la sentencia que la conducta del trabajador accidentado fue «clamorosamente imprudente»: que cabía pensar que podía haber declinado «realizar el trabajo encomendado» y, en todo caso, adoptar «las medidas precautorias adecuadas en evitación de un resultado lesivo para el mismo, incluidas las de ayudarse de otro u otro trabajador de tal manera que garantizase la sujeción de aquél o, en caso de caída, que el mismo no se precipitara al vacío».

[22] SAP de Barcelona n. 665/2003, cit., conocida por su dudosa aplicación de la herramienta de la autopuesta en peligro, absuelve a los empresarios de un delito grave de lesiones, que provocó al trabajador una tetraplejia al caer por un hueco al no haber ninguna medida de seguridad. La audiencia argumenta su posición sosteniendo que la postura imprudente del trabajador no se puede negar justificando que los empresarios no habían proporcionado medidas de seguridad, ya que fue el trabajador quien utilizó un caballete que se encontraba fortuitamente cercano al hueco por donde cayó sin ningún tipo de protección, cometiendo una acción claramente imprudente. Por lo que carece de relevancia el hecho de que haya quedado probado que los empresarios incumplen el deber de vigilancia, siendo lo relevante que es el trabajador quien voluntariamente omitió la norma de cuidado más básica. De esta forma se incurre en un importe error al ignorar las peculiaridades de la relación laboral y de la posición que ocupan cada una de las partes

apreciar la concurrencia con la autopuesta en peligro del trabajador[23]. Y, por último, nos encontramos con sentencias en las que la conducta del trabajador solo exonera al empresario cuando éste ha cumplido con todas sus obligaciones y la imprudencia del trabajador sea grave, imprevisible y suficientemente relevante[24].

Como se ha insistido anteriormente, la trascendencia de la conducta de la víctima ha de ser relativizada por cuanto no podemos olvidar el contexto en el que se desarrolla, en la posición del empresario respecto del trabajador y en el carácter subsidiario en el cumplimiento de las medidas de seguridad que el propio legislador atribuye al trabajador[25].

Hay que tener en cuenta que la obligación del empresario consiste en adoptar todas las medidas necesarias, lo que incluye necesariamente la exigibilidad de una determinada conducta del trabajador y la vigilancia y control de la misma.

El trabajador también viene obligado a cumplir con los sistemas de seguridad previstos en la empresa[26]. Ahora bien, es habitual que en el desarrollo de la actividad laboral se produzca una relajación cuya consecuencia es el uso de las dinámicas de trabajo seguras, por rutina o por obtener un mayor rendimiento en la actividad. Ello, en ocasiones, da lugar a accidentes, que ponen al descubierto en muchos casos deficiencias en la planificación o ejecución de las medidas de seguridad. Por tanto, al establecer éstas deben prevenirse, en lo posible, las conductas inadecuadas de los trabajadores.

Es por esa razón por la que, partiendo del concepto de imprudencia se pueden evaluar tanto el cumplimiento de las obligaciones preventivas del empresario, generales como especiales y su objetivo deber de cuidado[27].

---

dentro de la misma. Obviando los incumplimientos del empresario SAP de Zamora n. 321/2003, de 31 de mayo. *Vid.* M. COBO DEL ROSAL, J. SANCHEZ-VERA GÓMEZ-TRELLEZ, *op. cit.*, p. 16; R.M. GALLARDO GARCÍA, *Protección jurídica de la vida y salud de los trabajadores. Derecho Penal. Derecho Administrativo sancionador*, Comares, 2016, pp. 190-191.

[23] SAP de Madrid n. 309/2015, de 5 de mayo, FJ 9 (ARP 2015/517).

[24] SAP de Cantabria n. 2038/2004, de 31 de marzo (ARP 2004/177); STS n. 1853/2001, de 17 de octubre, FJ 1 y 4 (RJ 2002/1200). *Vid.* I. OLAIZOLA NOGALES, *Delitos contra los derechos de los trabajadores (arts. 316 y 317 CP) y su relación con los resultados lesivos*, en *InDret*, 2010, n. 2, pp. 32-33; J.A. LASCURAÍN SÁNCHEZ, *op. cit.* En este caso se estaría hablando de una compensación de culpas, y normalmente se llevan al ámbito de lo civil teniendo poco recorrido en el ámbito penal.

[25] Arts. 5.b TRET («cumplir lo previamente adoptado»), 29 LPRL y 14.4 LPRL (otros sujetos, pero siempre responsable el empresario).

[26] Sobre el contenido de los arts. 29 LPRL y 5.b TRET, *vid.* J. GORELLI HERNÁNDEZ, *Responsabilidad del trabajador por incumplimiento de sus obligaciones preventivas: el caso de la construcción*, en A. MONGE FERNÁNDEZ (dir.), *op. cit.*, pp. 172-196.

[27] Deber de seguridad del empresario de impedir las conductas imprudentes del

La infracción de este deber junto a la falta de previsión de conductas imprudentes leves provocadas por la habituación al riesgo, o por el desarrollo de trabajos monótonos o repetitivos desplazan los límites del riesgo permitido elevándolos y dificultando con ello una posible exoneración de responsabilidad del empresario[28].

4. La IA, la IoT y el poder del empresario

La existencia de una conducta imprudente del trabajador a través del análisis de los elementos de la imprudencia puede llegar a incidir directamente sobre el grado de cumplimiento de las obligaciones preventivas del empresario.

La utilización de las nuevas tecnologías por parte de los empresarios hace que la gestión, la organización o la producción sean más eficientes y, probablemente más competitiva pero, también limita y condiciona el poder de dirección del empresario, paradójicamente más amplio, en cuanto vigilancia y control, pero más limitado en su haz de facultades, ya que generalmente depende directamente de la tecnología, siendo ésta, en un importante número de ocasiones, quien condiciona el propio proceso productivo[29].

La nueva era digital, IA o IoT, parece estar subordinando la actividad económica y productiva de la empresa a su propia iniciativa sin que hasta el momento parezca que se estén adoptando las medidas necesarias para no perder este control[30].

---

trabajador hacia sí mismo o hacia otros. El deber de cuidado que la cadena de mando de la empresa asume en cuanto garantes de la indemnidad del trabajador, alcanza no sólo en su actuación ordinaria sino incluso cuando ésta llega a ser descuidada por la confianza y la rutina. *Vid.* J.A. LASCURAÍN SÁNCHEZ, *op. cit.*, p. 566.

[28] No se trataría tanto del criterio del riesgo cuanto determinar si el resultado producido «encaja o no en el fin de la protección de la norma» (G.A. VALLEJO JIMÉNEZ, *Aproximación al concepto de imprudencia*, en *Nuevo Derecho*, 2010, vol. 5, n. 6, p. 35; *cfr.* también J.A. LASCURAÍN SÁNCHEZ, *op. cit.*, pp. 566 y 586-591).

[29] Se está produciendo una nueva "dependencia tecnológica" (C. SÁNCHEZ-RODAS NAVARRO, *Poderes directivos y nuevas tecnologías*, en *Temas Laborales*, 2017, n. 138, p. 165; *vid.* también J.R. MERCADER UGUINA, *La robotización y el futuro del trabajo (1)*, en *Trabajo y Derecho*, 2017, n. 27, pp. 14-15).

[30] En la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), se recogen, entre otros principios éticos dentro de los relacionados con el *desarrollo de la robótica y la inteligencia artificial para uso civil*, como la primacía de los derechos humanos sobre el uso de la robótica (§ 10) o la previsión normativa dentro de la UE de «un código de conducta para los ingenieros en robótica, un código

La subordinación del empresario a la tecnología va a tener una trascendencia muy importante en el ejercicio de su poder de dirección, sobre todo desde la perspectiva del control y vigilancia de la actividad de sus trabajadores. Pero también la va a tener sobre el cumplimiento de sus obligaciones para con ellos, centradas principalmente en las relativas a la protección de su salud.

La obtención de datos a través, entre otras, de las medidas de vigilancia y control de la actividad, sitúa al empresario, paradójicamente, en una posición del conocimiento "pleno" sobre los riesgos que genera y sobre los que se derivan de la conducta de sus trabajadores en la prestación de su servicio. Este conocimiento debería dificultar considerablemente, por injustificada, una posible inacción ante las deficiencias observadas en la protección eficaz de la salud de sus trabajadores.

El Tribunal Constitucional, en distintas sentencias no exentas de polémica, enmarca de forma recurrente el uso de la tecnología dentro del haz competencial del empresario[31] justificando lo que, en ocasiones parece injustificable, en oposición a los derechos de los trabajadores. La identificación de estas tecnologías como recursos y medios de la actividad empresarial parece otorgar un control pleno sobre su uso al empresario sin que con ello se entiendan vulnerados los derechos de los trabajadores en caso de colisión[32] [33].

---

deontológico destinado a los comités de ética de la investigación para la revisión de los protocolos de robótica, y licencias tipo para los diseñadores y los usuarios» que se desarrolle dentro de «un marco ético claro, estricto y eficiente» (§ 11). Todos ellos bajo el prisma del «principio de transparencia, que consiste en que siempre ha de ser posible justificar cualquier decisión que se haya adoptado con ayuda de la inteligencia artificial y que pueda tener un impacto significativo sobre la vida de una o varias personas; considera que siempre debe ser posible reducir los cálculos del sistema de inteligencia artificial a una forma comprensible para los humanos; estima que los robots avanzados deberían estar equipados con una "caja negra" que registre los datos de todas las operaciones efectuadas por la máquina, incluidos, en su caso, los pasos lógicos que han conducido a la formulación de sus decisiones» (§ 12). Sobre las directrices éticas en materia de IA, *vid.* la comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Generar confianza en la inteligencia artificial centrada en el ser humano*, COM(2019)168 final, 8 abril 2019.

[31] STC n. 66/2002, de 21 de marzo, FJ 7. *Vid.* M.C. AGUILAR DEL CASTILLO, *El uso de la tecnología y el derecho de huelga: realidades en conflicto*, en *Labour & Law Issues*, 2018, vol. 4, n. 1, C., pp. 1-30.

[32] Entre otras sentencias polémicas en cuanto se ven implicados derechos constitucionales *vid.* la STC n. 39/2016, de 3 de marzo (en *BOE*, 8 abril 2016), sobre el derecho de protección de datos de los trabajadores, la STC n. 17/2017, de 2 de febrero (en *BOE*, 10 marzo 2017), sobre el esquirolaje tecnológico, la STC n. 119/2014, de 16 de julio (en *BOE*, 15 agosto 2015), o la STC n. 8/2015, de 22 de enero (en *BOE*, 24 febrero 2015). Cada vez con mayor frecuencia parece como si los derechos constitucionales

Los poderes del empresario derivados de su derecho de libertad de empresa son muy amplios y abarcan multitud de facetas, entre las que se incluyen todas aquellas que afectan a la prestación de trabajo, ya sea en su relación con el trabajador a través del poder de dirección, como en la organización del proceso productivo en el que la relación laboral se desarrolla[34]. Consideramos necesario recordar que el poder de dirección del empresario, entendido como la capacidad que tiene de ordenar el modo, tiempo y lugar de la ejecución del trabajo, no es un fin en sí mismo, sino que es uno de los poderes que le permite la autotutela de sus intereses y que está formado por un conjunto de potestades entre las que se encuentra el poder de vigilancia y control y el poder en la ejecución de la prestación laboral[35]. Por ello cualquier alteración que se produzca en la organización de los recursos materiales de la empresa pueden llegar a afectar, con mayor o menor intensidad, a la prestación de trabajo en general y a la protección de la salud del trabajador en particular.

La automatización de puestos de trabajo o su sustitución por tecnologías denominadas como "inteligentes" se entiende como una necesidad de cambio y de adaptación a las nuevas exigencias del mercado. Las razones que llevan a una empresa a su adquisición pueden ser diversas: económicas, organizativas o cualesquiera otras. En todo caso, todas constituyen argumentos perfectamente válidos, que se resumen como un ejercicio del haz competencial del empresario que, en todo caso, no tiene porqué justificar.

La metamorfosis que está sufriendo nuestra sociedad afecta al funcionamiento normal, si con ello entendemos un proceso productivo tradicional, de nuestras empresas. Su digitalización a través de la tecnología de procesamiento de datos, software inteligentes y sensores

estuvieran cediendo ante el mayor poder del empresario en su potestad de organización y dirección de la actividad productiva, creándose una "irreal" creencia sobre una posición de igualdad entre los sujetos dentro de la relación laboral. *Vid.* STEDH n. 1874/13 y n. 8567/13, de 9 de enero de 2018, caso *López Ribalda y otros* c. *España*, sobre el incumplimiento de información necesaria en el derecho sobre la protección de datos.

[33] *Vid.* M.C. AGUILAR DEL CASTILLO, *La protección de datos entre el contenido constitucional y su contenido legal*, en *Labour & Law Issues*, 2016, vol. 2, n. 1, I., pp. 28-43; C. SÁNCHEZ-RODAS NAVARRO, *op. cit.*, p. 177; S. RODRÍGUEZ ESCANCIANO, *Las nuevas relaciones laborales en las empresas digitales y el control empresarial*, en C. GARCÍA NOVOA, D. SANTIAGO IGLESIAS (dirs.), *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Aranzadi, 2018, pp. 563-568.

[34] C. SÁNCHEZ-RODAS NAVARRO, *op. cit.*, p. 167.

[35] Y. SÁNCHEZ-URÁN AZAÑA, M.A. GRAU RUIZ, *El impacto de la robótica, en especial la robótica inclusiva, en el trabajo: aspectos jurídicos-laborales y fiscales*, en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2019, n. 50, p. 18.

permite predecir, controlar, planear y producir de forma inteligente[36], pero también facilita la adecuación de las decisiones adoptadas sobre la eliminación o reducción del riesgo en el desarrollo de todo ese proceso. La revolución 4.0, además de otras cuestiones, ha cambiado el qué y cómo hacer las cosas y esto necesariamente va a afectar a la protección de la salud de los trabajadores.

5. Información "inteligente" al servicio de la prevención

La incorporación de las tecnologías "inteligentes" en la organización de la empresa e incluso, en el proceso de toma de decisiones del empresario plantea dos cuestiones importantes desde el punto de vista de la prevención de riesgos laborales: la primera ¿si, en todo caso, ha de formar parte de sus funciones? Y la segunda, si la respuesta es afirmativa, ¿cuál ha de ser su nivel de afectación?

5.1. La prevención de los riesgos laborales como contenido de la IA

Sobre la pregunta de ¿si la prevención, en todo caso, ha de formar parte de las funciones de la IA? La respuesta vendrá dada por una condición, que dependerá de su incidencia sobre los riesgos de la empresa y su protección. Hay que tener en cuenta que, ostentar la posición de garante de la seguridad de los trabajadores dentro de la empresa no es una decisión voluntaria sobre la que el empresario pueda optar. Constituye una obligación inherente a su propio poder[37] que despliega todos sus efectos jurídicos cuando se ejerce dentro de la relación laboral[38]. El contenido y alcance de esta obligación dificulta, cuando no impide, deslindar los poderes empresariales de organización y de dirección en la utilización de los medios de los que dispone cuando pueden afectar a la protección de la salud de los trabajadores.

La integración como elemento definitorio del contenido de la obligación de seguridad[39] significa que su cumplimiento «debe proyectarse en los

[36] Aunque referido a la Revolución 4.0 en general, su trasposición a la empresa y al cumplimiento de las obligaciones preventivas solo es una manifestación del cambio tecnológico producido. *Vid.* S. BARONA VILAR, *op. cit.*, p. 22.

[37] M.T. IGARTUA MIRÓ, *op. cit.*, pp. 139-141.

[38] *Ibidem*, pp. 142-143.

[39] Una de las consecuencias más importantes de la reforma legal de la LPRL realizada por

procesos técnicos, en la organización del trabajo y en las condiciones en que éste se preste»[40]. Para ello deberá cumplir con «todas las obligaciones establecidas en la normativa sobre prevención de riesgos laborales»[41], adoptar cuantas medidas sean necesarias para su garantía e integrar en ella a todos los niveles jerárquicos de la empresa[42].

La claridad de la obligación de seguridad queda condicionada por la concreción de su contenido. La necesidad de «adoptar cuantas medidas sean necesarias» puede, en ocasiones, llegar a constituir un elemento disuasorio en el cumplimiento de la norma o, un mero cumplimiento formal de la misma. Por ello, el plan de prevención como «la herramienta que integra la actividad preventiva de la empresa en su sistema general de gestión y establece su política preventiva»[43] no puede obviar, para su elaboración, el contar con todos los medios existentes en la empresa, aunque no se hayan adquiridos con esa función, finalidad o intencionalidad.

Cuando los medios utilizados tienen software de IA o forman parte de la IoT serán relevantes siempre que puedan afectar directa o indirectamente a la identificación, evaluación o gradación de los riesgos, a la previsión de conductas peligrosas o a cualesquiera otros aspectos que guarde relación con la prevención de los riesgos laborales. Y todo ello por la posición de garante de la seguridad que la LPRL[44] atribuye al empresario.

Por otro lado, el carácter dinámico y permanente de la obligación de seguridad demanda que, ante cualquier modificación o adaptación tecnológica que se produzca en la empresa, se ha de tener en cuenta su incidencia en la prevención de los riesgos de la misma y, en función de ellas, desarrollar el procedimiento preventivo previsto en la norma. Hablar de la incidencia de las nuevas tecnologías en la prevención presenta dos aspectos que, formando parte de un todo, adquieren una trascendencia

---

la Ley 54/2003 es la reforzar la posición del plan de prevención como herramienta a través de la cual se ha de integrar la prevención de los riesgos en «el sistema de gestión de la empresa, en el conjunto de todas sus actividades y en todos sus niveles jerárquicos a través de la su implantación y aplicación» (art. 1, RD 39/1997).

[40] Art. 1.1, RD 39/1997.

[41] Art. 14.3 LPRL, teniendo en cuenta, según se prevé en el art. 1 LPRL, que tendrá la consideración de normativa sobre prevención de riesgos laborales todas las contenidas en la LPRL, «sus disposiciones de desarrollo o complementarias y cuantas otras normas, legales o convencionales, contengan prescripciones relativas a la adopción de medidas preventivas en el ámbito laboral o susceptibles de producirlas en dicho ámbito».

[42] Art. 1.1, RD 39/1997, atribuyéndoles la obligación «de incluir la prevención de riesgos en cualquier actividad que realicen u ordenen y en todas las decisiones que adopten».

[43] Art. 2.1, RD 39/1997.

[44] Art. 14.1 LPRL.

diferente si afectan directamente a un puesto de trabajo, alterando sus condiciones o robotizándolo o se insertan en el proceso de toma de decisiones de la empresa. El primero de los supuestos no presenta ninguna especialidad puesto que nos encontraríamos ante la obligación de realizar una evaluación sucesiva de los posibles riesgos que puedan generarse respecto de la evaluación inicial[45]. El segundo supuesto, tampoco afectaría a la obligación de seguridad por cuanto, aunque la actividad o el mismo puesto de trabajo se mantenga, la prestación queda automatizada o la suple un robot, en cuyo caso el riesgo desaparece en la medida en la que lo hace el sujeto que puede estar afectado por el mismo. La tercera opción sí puede llegar a plantear mayores problemas, en la medida en la que su funcionalidad se define por la emisión de "decisiones" a través de la obtención de datos. Atendiendo a su finalidad, si estas "decisiones" afectan a la organización de la actividad total o parcialmente y son incorporadas por el empresario a su proceso decisional, entendemos que también quedan integradas en su obligación de seguridad.

5.2. La prevención de los riesgos, el tratamiento de los datos y el nivel de complejidad de la IA

La accesibilidad cada vez mayor de tecnologías "inteligentes" por parte de las empresas puede hacer de la prevención de riesgos laborales una asignatura a la que se le presta menos atención. El cumplimiento meramente formal de la obligación de seguridad del empresario puede quedar superado por la incorporación de estas tecnologías a la organización de la empresa.

Las TICs, la IoT e incluso la IA como tecnologías disruptivas son fuentes inagotables de datos que, aunque no generan resultados por sí solos, su procesamiento para su traducción en respuestas o soluciones legibles facilitan la automatización de procesos, reformulan procedimientos y condicionan las decisiones empresariales buscando, principalmente, la eficiencia y la eficacia de la actividad, siempre en interés de la propia empresa.

Aunque toda la información que se puede llegar a obtener no supone una innovación en sí misma, la utilización de sus resultados por la empresa sí puede llegar a optimizar los medios con los que cuenta. Si nos acercamos

[45] Art. 4.2.a, RD 39/1997. *Vid.* V. MARTÍNEZ, Á. DE LA RÚA, *Mi compañero de trabajo es un robot*, en *El Pais.com*, 15 noviembre 2019.

al concepto de evaluación de los riesgos, como instrumento esencial para la gestión y aplicación del plan de prevención[46], se observa cómo la información se erige en el núcleo central sobre el que ha de recaer toda la prevención ya que, a partir de ella se identifican, evalúan y califican, en función de su peligrosidad, los riesgos y se toma la decisión sobre cuáles son las medidas más idóneas a adoptar[47].

La indiscriminación de los riesgos hace que toda la información obtenida por la empresa pueda ser relevante para la protección del trabajador con independencia de su procedencia. Esto no implica, no obstante, que toda ella ocupe el mismo lugar de prioridad en cuanto a su eficacia. Es necesario conocer de dónde se extraen los datos y su algoritmo de procesamiento y análisis para determinar su idoneidad y adecuación con los resultados que se obtienen.

La procedencia de la información puede ser muy variada y, superada la tradicional distinción entre datos personales y no personales, se ha establecido otra nueva clasificación más acorde con la realidad del big data[48] en la que se distingue entre «datos voluntarios, datos observados y datos inferidos»[49]. La diferencia principal entre los dos primeros se encuentra en su procedencia real, es decir, si han sido facilitados directamente por la persona, en el primer caso y los deducidos del análisis de comportamientos en el segundo. Así los datos observados «son medidos por maquinaria de software» que extrae y comparte los datos

---

[46] Art. 16.2 LPRL.

[47] Art. 3.1, RD 39/1997: «La evaluación de los riesgos laborales es el proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse».

[48] «Llamamos *Big data* al almacenamiento, tratamiento y transferencia de datos a gran escala» (M. SANCHO LÓPEZ, *Internet, Big data y nuevas tecnologías: repercusiones y respuestas del ordenamiento jurídico*, en *CEFD*, 2019, n. 39, p. 309) y se define por sus tres uves, aunque no es necesario que se den las tres: «*Big data* is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation» (*Big Data*, en *Gartner Glossary*).

[49] M. HILDEBRANDT, *Esclavos de los macrodatos. ¿O no?*, en *IDP*, 2013, n. 17, p. 14. Otra posible clasificación sería la de hablar de «datos estructurados, aquellos que provienen de fuentes de información conocidas y que, por tanto, son fáciles de medir y analizar en los sistemas tradicionales, en contraposición a lo que se ha dado en llamar datos no estructurados. […] teniendo en cuenta la variedad de su origen, así como la rapidez con que se incrementa su volumen, ha sido necesario el desarrollo de nuevos modelos de software para adecuarse a su carácter disperso y heterogéneo» (M. SANCHO LÓPEZ, *op. cit.*, p. 310).

para obtener los datos inferidos[50].

Referirnos a maquinaria de software nos conecta con la denominada internet de las cosas (IoT) que puede definirse como «todo objeto físico o dispositivo inteligente, con capacidades de computación, es decir que dispone de electrónica y/o de un ordenador embebido, y con capacidades de interconexión con redes de datos, ya sean internas, como en la empresa o entorno industrial o a Internet. Incluye la agrupación y trabajo coordinado de estos en diversos entornos»[51].

Junto a estos entornos conviven otras tecnologías como las ponibles o webrables, e incluso otras que, con una filosofía similar, están pasando a integrarse directamente en el cuerpo humano a través de microchips y que se denominada tecnología inyectable[52]. Todas ellas facilitan información que puede estar interconectada, lo que facilita crear patrones de comportamiento, «una especie de inteligencia colectiva que se incorpora a las cosas conectadas mediante modificaciones de su software e instrucciones de funcionamiento»[53]. «Esta conciencia colectiva se usa como base de aprendizaje de algoritmos e inteligencias artificiales para mejorar el software de los elementos (IoT) y su capacidad para interpretar el entorno»[54].

De forma más compleja el proceso de la IA también va a extraer conclusiones en base a los datos recibidos, aunque en este caso nos encontramos ante «unas cifras de datos difícilmente legibles que, cada vez con mayor rapidez se están retroalimentando y extrayendo, de forma autónoma, conclusiones que con frecuencia escapan a la conciencia de la persona que originariamente las diseñó. Con la utilización de la IA se trata de establecer una especie de correlación a través de la ejecución de un gran número de algoritmos sobre los datos obtenidos, para en una segunda fase diseñar algoritmos específicos para su aplicación a casos concretos. En la primera fase se piensa con los datos y en la segunda se actúa sobre ellos, en estos casos el sistema aprende cuales son los criterios relevantes de análisis de datos (machine learning o aprendizaje profundo) y clasifica los datos por capas lo que a veces hace que sea muy difícil entender las razones de un resultado»[55]. Estamos entrando en un bucle en el que los datos se alimentan a sí mismos haciendo cada vez más difícil su

---

[50] M. HILDEBRANDT, *op. cit.*, p. 14.

[51] «Son cosas que sientes, actúan y se comunican» (P. LLANEZA GONZÁLEZ, *Seguridad y responsabilidad en la Internet de las cosas (IoT*), Wolters Kluwer, 2018, p. 21).

[52] A. BERNARDO, *De la tecnología wearable a la inyectable*, en *Blogthinkbig.com*, 11 junio 2015.

[53] P. LLANEZA GONZÁLEZ, *op. cit.*, p. 22.

[54] *Ibidem*, p. 23.

[55] *Idem*.

control y su predictibilidad.

Con el tratamiento de los datos[56] a través de su algoritmización se transforma un contenido ilegible en patrones de comportamiento, lo que favorece la mecanización de multitud de procesos y la previsibilidad de conductas[57]. El estudio y análisis de estos patrones pueden llegar a formar parte de la evaluación de los riesgos por cuanto la información obtenida favorece el control periódico de las condiciones de trabajo, de la organización y los métodos de trabajo, así como del estado de salud de los trabajadores[58]. Hay que tener en cuenta, no obstante, que una decisión tomada con base exclusiva en cálculos algorítmicos no puede otorgársele un carácter científico, ya que si bien la obtención de datos puede considerarse neutral no lo es su procesamiento que se hará en base al procedimiento matemático o estadístico del algoritmo o algoritmos que se hayan utilizado. El contenido del algoritmo siempre va a depender de la voluntad de quien lo diseña o de quien lo solicita en función de sus propios intereses[59].

---

[56] Art. 4.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos): se entiende por «"tratamiento": cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

[57] «Este *Big data* es la realidad del siglo XXI y a través de la misma el mundo que se ofrece es el de la predicción y con ella la predictibilidad de muchos componentes vitales. Son los ojos que ven al mundo y los ojos desde los que se mueve el mundo» (S. BARONA VILAR, *op. cit.*, p. 26).

[58] Art. 1.b, RD 39/1997. Se trata de orientar el análisis de los datos a la evaluación de los riesgos y a la protección de la salud. *Vid.* R. GALINDO CALDÉS, *Big data e inteligencia artificial en la gestión de los recursos humanos del sector público*, en Revista Catalana de Dret Públic, 2019, n. 58, p. 53.

[59] «Si bien los algoritmos se atienen a una lógica científica-matemática, la forma en que éstos son proyectados al estudio de los procesos sociales responde indudablemente a unas coordenadas ideológicas concretas y, por tanto, existe cierto riesgo de que se produzca un proceso reduccionista y simplificador de etiquetaje respecto de determinados colectivos» (M. SANCHO LÓPEZ, *op. cit.*, p. 313). La transparencia en estos procesos se erige como un principio de protección frente a la IA, dentro de los *Requisitos esenciales para una IA fiable* (COM(2019)168 final, cit., § 2.2, punto IV). *Vid.* S. RODRÍGUEZ ESCANCIANO, *op. cit.*, pp. 563-568.

6. Los datos como fuente de información de la evaluación de riesgos

La elaboración de un plan de prevención demanda un conocimiento profundo de la actividad a evaluar y de la idiosincrasia de cada uno de los puestos de trabajo que la conforman. Se trata de datos cuasi objetivos que, después de casi veinticinco años de vigencia de la LPRL están recogidos en los distintos planes de prevención existentes.

Hablar de los riesgos de una determinada empresa nos dirige directamente al sector de producción al que pertenece, a su normativa reguladora y a todas aquellas medidas que le afectan y que pueden encontrarse en fuentes de muy diversa índole: jurídicas, institucionales o profesionales. Todas ellas con acreditada solvencia en la identificación de los riesgos, en su calificación en cuanto a su intensidad y en las medidas a adoptar para eliminarlos o reducirlos. Toda la información proveniente de estas fuentes tiene como denominador común que van a identificar los riesgos y sus medidas preventivas objetivamente, es decir, que van a ser comunes a todas las empresas que desarrollen la misma actividad. Esta homogeneidad no implica que todas ellas tengan los mismos riesgos, sino que en aquellos en los que coinciden, su evaluación y las medidas a adoptar van a ser idénticos. Procesar esta información con la tecnología actual implica un bajo nivel de dificultad, dada la capacidad de datos que en milésimas de segundo se pueden llegar a analizar, y un bajo coste, si tenemos en cuenta la utilidad que puede llegar a generar.

Sin negar la utilidad evidente de los resultados procesados a partir de la obtención de los datos anteriores, no hay que olvidar que la empresa es un ente vivo que necesita de una individualización en el análisis de sus riesgos. Y, este solo puede proceder de la obtención de nuevos datos derivados, entre otros, del entorno donde se desarrolla la actividad, de los riesgos generales de la empresa y de los propios derivados del puesto de trabajo tanto de carácter objetivo como subjetivo. Centrándonos solo en los derivados del puesto de trabajo y en los de carácter subjetivo, los riesgos y la obtención de la información necesaria para combatirlos provendrá de la organización del trabajo, de las características del trabajador, de las condiciones en las que se desarrolla la prestación de trabajo y de su conducta.

La capacidad de control que permiten y facilitan las nuevas tecnologías está dando como consecuencia lo que se ha denominado un "trabajador de cristal"[60] por cuanto toda su actividad puede quedar registrada

[60] C. SÁNCHEZ-RODAS NAVARRO, *op. cit.*, p. 173.

milimétricamente durante todo su tiempo de trabajo. La sofisticación de las medidas de videovigilancia o del control que imponen las maquinas en el desarrollo de la actividad dejan muy poco margen de autonomía al trabajador y fortalece el nivel de control del empresario.

La neutralidad de los datos desaparece cuando son procesados. Es durante su análisis y tratamiento donde se introduce el sesgo deseado y se obtiene el resultado esperado. En la empresa, será la voluntad del empresario la que determine qué datos son los relevantes, entre toda la información obtenida, y cuáles no. Por eso eliminar el sesgo preventivo de los mismos no va a afectar al grado de cumplimiento de su obligación, pero sí puede llegar a tenerse en cuenta en la valoración que se haga de la conducta del trabajador en la eliminación o disminución de alguna de sus responsabilidades.

En la obtención y tratamiento de la información es la IA la que, en función de su programación, decide si se centra en el control de la actividad o extiende este análisis a las condiciones de trabajo y a cómo afectan a la salud y seguridad del trabajador. La información puede ser la misma, pero el resultado será diferente. Se trata de poner la tecnología al servicio de la prevención de los riesgos laborales, sin perjuicio de que también lo esté al del control de la prestación de trabajo. El carácter finalista de estas tecnologías no va a verse afectado por la concurrencia de procedimientos matemáticos diversos.

7. La información como requisito en la obtención de datos

Como la información obtenida por el empresario va a depender del resultado de su supervisión y de la vigilancia y control a la que se somete al trabajador en su prestación de trabajo, el cómo ejerza este poder de dirección va a tener una trascendencia importante en la posición deudora que ocupa frente al trabajador.

Sin entrar a valorar los evidentes riesgos a los que se expone el trabajador en la defensa de derechos fundamentales como los de intimidad o protección de datos[61] cuando entran en colisión con el derecho del empresario de libertad de empresa, hay que señalar que la existencia de un vínculo contractual laboral es suficiente para entender prestado el consentimiento[62], no así la obligación de informar sobre la existencia de

[61] Art. 18 CE.

[62] *Vid.* el considerando 32 del Reglamento (UE) 2016/679, cit.: «El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de

herramientas tecnológicas como las de videovigilancia, que debe facilitarse «con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida» (art. 89.1, Ley Orgánica de Protección de Datos Personales (LOPDP))[63] y de su finalidad. Esta obligación no es extensible a los procesos de organización de la actividad a no ser que los medios utilizados ejerzan un control directo sobre la prestación de trabajo.

La LOPDP en su art. 89.1 establece que «los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Lo que implica que la incorporación de entornos inteligentes en la empresa para procesar, transmitir y tratar los datos obtenidos, ya sean voluntarios u observables, no va a afectar directamente a la obligación de seguridad del empresario, pero sí a su cumplimiento, los haya o no previsto. Téngase en cuenta que quién toma la decisión sobre la finalidad que se persigue con estos medios es el empresario por lo que, siendo consciente de su potencialidad en la determinación de los riesgos, no hacerlo puede llegar a cuestionar el cumplimiento del objetivo deber de cuidado que le es exigible.

La afirmación anterior no implica que el empresario se encuentre en la obligación de adquirir la tecnología más puntera para su empresa, pero sí que incorpore todas las potencialidades que se derivan de los medios tecnológicos con los que ya cuenta al cumplimiento de este deber.

8. El "riesgo permitido", la conducta del trabajador y la IA

Los resultados obtenidos a través de la IA con el tratamiento de todos los datos relacionados con los riesgos que pueden derivarse de una actividad, sobre todo los datos inferidos, pueden llegar a identificar todos aquellos riesgos que, una vez adoptadas todas las medidas de seguridad y sin una actuación previa del empresario, superan el umbral de "riesgo permitido". Es decir, que cualquier conducta del trabajador que generase un riesgo por debajo de este umbral debería ser considerada como una imprudencia

carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal»; art. 4.11.

[63] Ley Orgánica 3/2018, de 5 de diciembre (en *BOE*, 6 diciembre 2018).

profesional, siempre que se demuestre que no se han adoptado todas las medidas necesarias para evitarlas.

Hay que tener en cuenta que todo control que se realiza a través de tecnologías e IA, IoT, de supervisión, como la videovigilancia, GPS, drones, o más personalizadas como los webrables, tecnología inyectable, de reconocimiento facial, control digital, entre otras muchas, no solo deben controlar el exacto cumplimiento de la prestación laboral sino que también han de contar con procedimientos matemáticos o estadísticos adecuados para el análisis de comportamientos o la elaboración de perfiles que permitan detectar riesgos a través de conductas que puedan superar los estándares del riesgo permitido cuando no se dispone de una información tan detallada[64].

Si el resultado de los datos inferidos es la previsión de conductas imprudentes por parte de los trabajadores, el empresario no puede permanecer al margen de la información obtenida a través de estas tecnologías amparándose en la, generalmente, anonimicidad de los datos obtenidos. La procedencia aparentemente inocente de los datos recabados en la empresa que no requieren consentimiento expreso, aquellos que aun exigiéndolo se entiende otorgado en el momento de la conclusión del contrato de trabajo[65] y la obligación de informar a los trabajadores sobre la

[64] Estaríamos dentro de lo que se denomina "agregación", es decir, se trataría de interrelacionar todos los datos obtenidos entre sí «para lograr aumentar exponencialmente la información a obtener y, de ese modo, sacarle un mayor partido» (M. SANCHO LÓPEZ, *op. cit.*, p. 311), se trata de conformar un perfil de riesgos o conductas, a través de la triangulación y organización de la información que se ha obtenido sobre ellos, generando nuevos datos sobre ellos y sobre todo sobre esas conductas.

[65] STC n. 39/2016, cit., FJ 3: «En el ámbito laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y cumplimiento del contrato firmado por las partes […] lo que abarca, sin duda, las obligaciones derivadas del contrato de trabajo». Según la STS n. 304/2019, de 10 abril, FJ 2.B.3, el consentimiento no es preciso conforme al art. 6.1.b del Reglamento (UE) 2016/679, cit., cuando «el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte», debiéndose entender por tratamiento la definición que da el citado art. 4.2 del Reglamento, que entiende por tal la simple recogida de un dato o cualquier operación sobre datos, sin que el tratamiento de datos se encuentre prohibido, como norma general del art. 9.1, cuando sea «necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social» (art. 9.2.b). Sobre la SAN de 15 de junio de 2017, casada y anulada con la sentencia anterior *vid.* E. GONZÁLEZ BIEDMA, *Derecho a la información y consentimiento del trabajador en materia de protección de datos*, en *Temas Laborales*, 2017, n. 138, pp. 236-244.

finalidad de los mismos cuando recae directamente sobre la prestación de su trabajo[66], generan una información lo suficientemente importante que, la ignorancia de sus resultados puede llegar a evidenciar una falta de control por parte del empresario, exigible en todo caso por su deber objetivo de cuidado.

Por otro lado, la anonimicidad de los datos obtenidos puede servir también de estrategia para la no identificación del trabajador expuesto a estos riesgos. Se puede caer en la tentación de justificar una posible inacción del empresario amparada en la falta de correlación existente entre un potencial peligro y el trabajador que pueda materializar el riesgo en un daño. La funcionalidad de la IA o de la IoT, no es personalista. Los datos que obtienen son agregados de distintas fuentes para conforman un determinado perfil, que con la organización de la información obtenida y su triangulación vuelve a generar nuevos datos[67] que, con la velocidad de su procesamiento y lo limitado de su espacio, resultan fácil de interpretar o de aplicar. Nos estamos refiriendo a una empresa que, por muy grande que sea, sus límites son finitos y, en todo caso perfectamente identificables a través de su propia estructura organizativa. Si no puede identificarse a priori al trabajador/es que desarrollan una determinada actividad, sí puede definir el puesto de trabajo y la conducta que genera el riesgo detectado, siendo fácil establecer la correspondiente relación[68] a través de la

[66] Según la citada STC n. 39/2016 «el incumplimiento del deber de requerir el deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada». En contra de esta afirmación el voto particular del Magistrado D. Fernando Valdés Dal-Ré al que se adhiere la Magistrada Dª Adela Asua Batarrita en el que se entiende que la ley solo excepciona de cumplimiento al consentimiento, pero que en ningún momento regula un tratamiento similar para el deber de información; en similar sentido, STC n. 292/2000, de 30 de noviembre. «Aceptar que el contenido del poder de dirección del empresario responde a esta exigencia significa tanto como otorgarle un carácter universal o sin apenas excepción en el marco del contrato de trabajo frente al derecho del trabajador vaciándolo de contenido y haciéndolo impracticable» (M.C. AGUILAR DEL CASTILLO, *La protección de datos entre el contenido constitucional y su contenido legal*, cit., p. 38; *vid.* también J. APARICIO TOVAR, *Los derechos fundamentales y el juicio de proporcionalidad degradados a mera retórica. A propósito de la STC 170/2013, de 17 de octubre de 2013*, en *Derecho Social*, 2013, n. 64, p. 136; M.B. CARDONA RUBERT, *Intimidad del trabajador y comunicaciones electrónicas según el Tribunal Constitucional*, en *Lex Social*, 2015, vol. 5, n. 2, p. 39).

[67] M. SANCHO LÓPEZ, *op. cit.*, p. 311.

[68] Art. 22.1 TRET: «Mediante la negociación colectiva o, en su defecto, acuerdo entre la empresa y los representantes de los trabajadores, se establecerá el sistema de clasificación profesional de los trabajadores por medio de grupos profesionales». Art. 22.4: «Por acuerdo entre el trabajador y el empresario se asignará al trabajador un grupo profesional y se establecerá como contenido de la prestación laboral objeto del contrato de trabajo la realización de todas las funciones correspondientes al grupo profesional asignado o

clasificación profesional de la empresa.
La evaluación de estos riesgos y las medidas a adoptar forman parte de la obligación del empresario, no porque provenga de una IA sino porque cuenta con la información y datos suficientes para constatar la existencia de esos riesgos generados por esas conductas.
La incorporación de tecnologías disruptivas en los procesos de toma de decisiones que afectan a la organización empresarial permite a las empresas optimizar sus recursos, pero, también incrementa su obligación de deber de cuidado para con sus trabajadores en una proporción inversa al alcance de la tecnología utilizada. Esta misma relación se produce entre el cumplimiento del deber de seguridad del empresario y la conducta imprudente no temeraria del trabajador en la medida en la que el nivel de riesgo permitido disminuye en la misma proporción en la que el empresario ejerce su poder de vigilancia y control sobre el trabajador.
Conocer la existencia del riesgo y no tomar las medidas preventivas necesarias entre las que se incluyen las órdenes e instrucciones impartidas, exime al trabajador del cumplimiento de sus propias obligaciones[69] en la medida en la que la relación de subordinación en la que se basa nuestro sistema de relaciones laborales prevé una obligación del trabajador de carácter subsidiaria en la que la exigibilidad de su cumplimiento solo es posible cuando haya recibido la formación preventiva adecuada y las instrucciones necesarias para ello[70].

9. La IA y la IoT: herramientas al servicio del empresario

La obligación de seguridad es una obligación de medios[71], por lo que tener capacidad para demostrar, al menos indiciariamente, que se han adoptado todas las medidas necesarias para evitar los riesgos puede constituir prueba suficiente para demostrar que se ha actuado con la diligencia debida y el daño se ha debido a factores imprevisibles para el empresario como puede ser una conducta temeraria del trabajador accidentado o de un compañero.
La existencia de un daño producido en la empresa hace recaer la carga de la prueba sobre el empresario que deberá demostrar que ha actuado con la

solamente de alguna de ellas».
[69] Art. 5.b TRET.
[70] Art. 29 LPRL; J. GORELLI HERNÁNDEZ, *op. cit.*, pp. 172-185.
[71] M.T. IGARTUA MIRÓ, *op. cit.*, pp. 146-147; A. DÍAZ MORENO, M.A. MARTÍN HUERTAS, *Aspectos fundamentales sobre responsabilidad y construcción en el ámbito civil*, en A. MONGE FERNÁNDEZ (dir.), *op. cit.*, pp. 344-348.

diligencia debida[72]. Esta obligación conlleva la eliminación o reducción del riesgo, mediante, entre otras, la adopción de medidas preventivas de carácter organizativo[73], la realización de controles periódicos de las condiciones de trabajo, la organización y los métodos de trabajo[74], la formación y la impartición de las órdenes e instrucciones precisas para el desarrollo de cualquier actividad. El cumplimiento de todas estas obligaciones implica desarrollar mecanismos adecuados de vigilancia y control sobre la conducta del trabajador en el desarrollo de su actividad, potestad que forma parte del poder de dirección del empresario[75].

De forma reiterada se argumenta por la jurisprudencia que «sería diabólico exigir al titular de la empresa el don de la ubicuidad para estar presente en todos los lugares en que se desarrollan actividades de peligro»[76]. Afirmación que alcanza todo su significado si nos referimos a medidas de vigilancia y control tradicionales, pero que hay que replantearse ante la irrupción de las nuevas tecnologías dentro de la empresa.

Siempre que se respeten los derechos fundamentales de los trabajadores, con la modelización propia de su ejercicio dentro de la relación laboral[77], sobre la utilización de la tecnología para controlar su actividad, hace ya mucho tiempo que la doctrina judicial y constitucional[78] avalan su

---

[72] Art. 96.2 LJS: «En los procesos sobre responsabilidades derivadas de accidentes de trabajo y enfermedades profesionales corresponderá a los deudores de seguridad y a los concurrentes en la producción del resultado lesivo probar la adopción de las medidas necesarias para prevenir o evitar el riesgo, así como cualquier factor excluyente o minorador de su responsabilidad. No podrá apreciarse como elemento exonerador de la responsabilidad la culpa no temeraria del trabajador ni la que responda al ejercicio habitual del trabajo o a la confianza que éste inspira». *Vid.* STS n. 149/2019, de 28 de febrero, FJ 4.3.B.

[73] Art. 3.1.a, RD 39/1997: «Eliminar o reducir el riesgo, mediante medidas de prevención en el origen, organizativas, de protección colectiva, de protección individual, o de formación e información a los trabajadores».

[74] Art. 3.1.b, RD 39/1997: «Controlar periódicamente las condiciones, la organización y los métodos de trabajo y el estado de salud de los trabajadores».

[75] Art. 20.3 TRET: «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad».

[76] STS n. 149/2019, cit., FJ 4; STS de 12 de julio 2007, RJ 2007\8226, FJ 2. Sobre la culpa "*in vigilando*" *vid.* J. GORELLI HERNÁNDEZ, *op. cit.*, pp. 228-229.

[77] STC n. 41/2006, de 13 de febrero, FJ 4, sostiene que «el ejercicio de las facultades organizativas del empleador no puede traducirse en la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni en la sanción del ejercicio legítimo de tales derechos por parte de aquél».

[78] Por todas, STC n. 39/2016, cit.; STC n. 29/2013, de 11 de febrero de 2013; STC n.

utilización como medios al servicio de los intereses de la empresa incardinados en el poder del propio empresario.

La supervisión, la vigilancia y el control al que puede someterse al trabajador a través de la utilización de tecnologías "inteligentes", de demostrada eficacia para los intereses de la empresa[79], da una significación diferente a la exigencia de los arts. 4.2, 12.A y 16.1 y 16.2 del Convenio OIT 155[80] en los que la adopción de medidas preventivas «razonables y factibles» dan contenido y establecen los límites de la obligación general de seguridad del empresario.

Los conceptos de razonabilidad y factibilidad como límite al contenido de la obligación de seguridad guardan una estrecha relación con los medios de los que dispone el empresario para organizar su actividad entendiendo que, en modo alguno, puede estar referidos a condicionantes económicos[81] sino solo a las posibilidades reales, en cuanto a su existencia y accesibilidad en el mercado, de todas las medidas preventivas necesarias para evitar los riesgos o disminuirlos. Es dentro de esta capacidad organizativa donde la IA o la IoT redefine los límites de la obligación de seguridad en dos direcciones, actuando sobre los riesgos derivados de la actividad, afectando directamente al contenido del plan de prevención de la empresa y sobre las conductas de los trabajadores a través de su vigilancia y control[82], siempre dentro del respeto a sus derechos

17/2017, cit.

[79] «Datificación, internet de las cosas y big data convergen sobre una base común de herramientas, tecnologías y procesos a gran escala que consolidan una tendencia a definir el modo en que las organizaciones o empresas tradicionales prestan sus servicios, entendidos en el nuevo contexto tecnológico como actividades dependientes de una infraestructura global de datos, de la que extraen conocimiento e información para desarrollar procesos críticos de su negocio, adoptar decisiones estratégicas y responder a la evolución de la competencia con un mejor control de los datos relevantes para su actividad» (M. MORENO MUÑOZ, *Privacidad y procesado automático de datos personales mediante aplicaciones y bots*, en *Dilemata*, 2017, n. 24, p. 9).

[80] En el Instrumento de Ratificación del Convenio OIT n. 155 sobre Seguridad y Salud de los Trabajadores y Medio Ambiente de Trabajo, adoptado en Ginebra el 22 de junio de 1981 (en *BOE*, 11 noviembre 1985), por ejemplo el art. 16.1 «impone a los empleadores, en la medida que sea razonable y factible, la obligación de garantizar que "los lugares de trabajo, la maquinaria, el equipo y las operaciones que estén bajo su control sean seguros y no entrañen riesgo alguno para la salud y seguridad de los trabajadores"».

[81] Se excluyen aquellas tecnologías de carácter auxiliar que no están incorporadas a la empresa, aunque puedan suponer una mejora para el bienestar de los trabajadores. En este sentido, Y. SÁNCHEZ-URÁN AZAÑA, M.A. GRAU RUIZ, *op. cit.*, pp. 16-17.

[82] STEDH de 17 de octubre de 2019, JUR\2019\289974, *López Ribalda y otros* c. *España*: «15.1. No se autorizará la introducción y el uso de sistemas y tecnologías de la información con el fin directo y principal de controlar la actividad y el comportamiento

fundamentales.

Como ya se ha insistido a lo largo del trabajo, hablar de IA o de la IoT es referirnos al tratamiento algorítmico de los datos, lo que nos lleva a mostrar una cierta cautela en sus resultados, sobre todo si se trata de analizar conductas. Las "decisiones" y "valoraciones" procedentes de esta tecnología no pueden tratase como verdades científicas irrefutables, entre otras razones porque cuentan con el mismo margen de error que el que se haya introducido en sus cálculos matemáticos. En el momento actual, la capacidad de "raciocinio" de las máquinas, por muy complejas que sean, viene determinado por algoritmos que necesitan ser traducidos, en el sentido que, por muchas variables que se utilicen, siempre podemos encontrarnos situaciones no contempladas que respondan a una conducta imprudente que, en un determinado entorno no lo sea o viceversa. Las máquinas "inteligentes" constituyen un diagnosticador de riesgos que necesita ser contextualizado. Son medios o instrumentos al servicio del empresario, de tal forma que su fiabilidad dependerá de la credibilidad que este le reconozca en función de su propia programación. Trasladar esta credibilidad a los trabajadores implica que reconozcan en la tecnología un poder de organización del que carece y al que difícilmente tienen acceso por formar parte de unos medios de producción cuya titularidad no ostentan.

En todo caso el uso de máquinas "inteligentes" implica incrementar la capacidad de control del empresario sobre el desarrollo de la actividad productiva, lo que conlleva entre otras cosas un control de los puestos de trabajo en tiempo real. Una de las características que definen a este control es la inmediatez de la reacción[83] lo que referido a situaciones de riesgo dificulta la capacidad del empresario para acreditar posibles causas de exoneración de su responsabilidad.

La deuda de seguridad del empresario se concibe en términos cuasiobjetivos por lo que contar con la información suficiente de la existencia de un riesgo cualquiera que sea su procedencia: directamente de la actividad productiva, de su organización o de la conducta de un

---

de los empleados. Cuando su introducción y utilización para otros fines legítimos, como la protección de la producción, la salud y la seguridad o para garantizar el funcionamiento eficaz de una organización, tenga como consecuencia indirecta la posibilidad de controlar la actividad de los trabajadores, debe estar sujeta a las salvaguardias adicionales establecidas en el principio 21, en particular la consulta a los representantes de los trabajadores. 15.2. Los sistemas y las tecnologías de la información que controlan indirectamente las actividades y el comportamiento de los trabajadores deben diseñarse y localizarse específicamente para no menoscabar sus derechos fundamentales».

[83] Se dice que «hacer ver es hacer sentir» en A. SCRIBANO, *Drones: una manera de ver*, en *Boletín Científico Sapiens Research*, 2017, vol. 7, n. 2, p. 71.

trabajador y, no actuar con la rapidez que los medios con los que cuenta permiten, implicaría un incumplimiento de su objetivo deber de cuidado.
No obstante, cuando la medida preventiva a adoptar consiste en una orden o instrucción, puede llegar a plantearse si la obligación se entiende cumplida cuando parte de una IA. Jurídicamente hablando entendemos que esta cesión no es posible porque el legislador solo reconoce al empresario el poder de dirección en el que se incluye esta potestad y, aunque prevé su delegación, esta solo puede recaer en personas físicas[84]. Y, por otro lado, la doctrina judicial y la de nuestro tribunal constitucional consideran a estas tecnologías como medios instrumentales al servicio del poder del empresario sin que puedan constituir un elemento de valoración en la posible vulneración de los derechos de los trabajadores.
No se trata de imponer al empresario la adquisición de medios técnicos más allá de las medidas preventivas exigibles tras una correcta evaluación de riesgos, sino de darle una finalidad preventiva además de la propia u originaria en los supuestos en los que ya existan en la empresa. Si tienen capacidad para ello, la programación de estas tecnologías también debe estar dirigida a la identificación de conductas peligrosas a través de la elaboración de patrones o perfiles genéricos que respondan a situaciones de riesgo reales, así como a la emisión de instrucciones sobre cómo proceder para evitar los daños que pueden generarse, información que queda integrada en el deber de seguridad del empresario y que le obliga a tomar decisiones con la urgencia que en cada caso se requiera. Como señala la STS de 8 de octubre de 2001 (RJ 2002/1424), «El deber de protección del empresario es incondicionado y, prácticamente, ilimitado. Deben adoptarse las medidas de protección que sean necesarias, cualesquiera que ellas fueran». No existe ningún precepto legal en el que

[84] SAP de Guipúzcoa, sección 1ª, sentencia n. 41/2012, de 3 de febrero, recurso 1210/2011, FJ 2.C.4: «La delegación no constituye un título por el que se transfiere la posición de garante. En virtud de la delegación no se transmite la responsabilidad en el tejido de seguridad. Lo que se modifica es el contenido del deber de garantía que ya no es realizar personalmente la tarea precisa para garantizar la seguridad exigible sino encargar la misma a una persona cualificada para tal fin – selección adecuada –, dotarle de los recursos necesarios para cumplir el objetivo exigido – dominio de la situación – y, finalmente, adoptar las medidas precisas para preservar que la persona a quien se encomienda la tarea realiza la misma de forma adecuada – control de la situación». *Vid.* A. MONGE FERNÁNDEZ, *op. cit.*, pp. 440-442 y 461-465. Muy interesante la transferencia de responsabilidad penal a la persona jurídica, pero siempre por actos de las personas físicas que actúan en beneficio de ella, en P. LLANEZA GONZÁLEZ, *op. cit.*, pp. 330-331. Todo ello al margen del debate sobre la posibilidad de dotar a los robots de una "personalidad electrónica" en la que los actos de los robots serían responsabilidad de ellos (Resolución del Parlamento Europeo, de 16 de febrero de 2017, cit.).

se exija al empresario la utilización de estas tecnologías, ni tan siquiera, cuando se encuentran perfectamente integradas en la organización. No obstante, sí existe una obligación genérica del empresario de proteger eficazmente la salud de los trabajadores. Si este objetivo se consigue con medios distintos a la IA o la IoT el empresario habrá cumplido con su obligación, pero solo siempre que obtenga el mismo nivel de protección que se alcanzaría con su utilización.

La exoneración de culpa por una conducta imprudente del trabajador será posible si el empresario es capaz de demostrar que, con todos los medios de los que dispone, no ha sido capaz de preverla o, era imposible hacerlo. El art. 14.2 LPRL establece que el empresario está obligado a adoptar cuantas medidas sean necesarias, por lo que, si cuenta con la tecnología suficiente para controlar el cumplimiento de la prestación de trabajo y abrir, en su caso, procedimientos sancionadores disciplinarios también deberá utilizarlos para la prevención de los riesgos laborales en la medida en la que son una condición de trabajo no jerarquizable respecto de las demás por lo que el uso de estas tecnologías no será exigible cuando pueda garantizar los mismos niveles de protección de la salud de sus trabajadores con la utilización de otros medios o medidas preventivas.

10. Conclusiones

Hablar de nuevas tecnologías en la actualidad se está convirtiendo en un eufemismo en la medida en la que lo nuevo se convierte en desfasado en un corto espacio de tiempo. Mas que referirnos a la capacidad de estas tecnologías hemos de centrarnos en las posibilidades que generan para el mundo de la prevención de riesgos laborales.

La obtención de datos a través de la mejora constante de las TICs, la IoT o la utilización, cada vez más frecuente de la IA en los procesos de producción permite a las empresas, a través de un tratamiento adecuado hacer más eficiente y competitiva su actividad productiva. Pero también incrementa el poder de dirección del empresario en cuanto a la vigilancia y control de la actividad de sus trabajadores.

A lo largo de todo el trabajo nos hemos centrado fundamentalmente en el tratamiento de los datos y en su relevancia en la obligación de seguridad del empresario, sobre todo como elementos de prueba para justificar una actividad diligente y una posible conducta imprudente del trabajador.

El empresario, como garante de la salud de sus trabajadores, está obligado a utilizar todos los recursos de los que su empresa disponga para el cumplimiento de esa obligación y, aunque preventivamente hablando,

consideramos que no es posible exigir al empresario la adopción de tecnologías como la IoT o la IA con el fin de proteger al trabajador. Entendemos que la implantación de estas tecnologías en la empresa, con independencia de su finalidad originaria, conlleva su inclusión en su obligación de seguridad.

La capacidad de control de estas tecnologías no se centra solo en la vigilancia de conductas sino en el tratamiento de todos los datos obtenidos. La algoritmización de cada vez un mayor número de procesos, no supone una subordinación aleatoria a las matemáticas, sino el cumplimiento de unos fines y objetivos predeterminados y exigidos a quién crea el algoritmo por parte de quien le contrata. En nuestro caso el empresario que es quien la adquiere como medio o instrumentos de organización de su actividad.

Dada su capacidad estas tecnologías pueden convertirse en una herramienta esencial para la identificación de los riesgos, su intensidad y su gravedad. También permite analizar las conductas de los trabajadores a través de los datos obtenidos en su control y los resultados de estas, lo que facilita la adopción de las medidas necesarias para evitarlas cuando puedan ser peligrosas para sí mismos o para el resto de los trabajadores, entre las que se deben incluir la impartición de las órdenes e instrucciones precisas.

La predicción de conductas imprudentes por la IA o la IoT debe generar en el empresario una respuesta inmediata que se traduzca en la adopción de medidas concretas sobre los riesgos o en la adopción de órdenes o instrucciones a los trabajadores para que desistan de esa conducta cuando no es posible la solución anterior. En este caso las distracciones e imprudencias no temerarias del trabajador pueden quedar muy limitadas cuando el empresario es consciente de su existencia. La imposibilidad de controlar una actividad en todo momento se reduce considerablemente cuando está monitorizada lo que significa que la posibilidad de control del empresario puede afectar tanto a la actividad productiva como a los riesgos derivados del trabajo siempre que así se prevea previamente. Es precisamente esta posibilidad la que crea una relación directamente proporcional entre el contenido de la obligación de seguridad del empresario con la capacidad tecnológica de control de su empresa e indirectamente proporcional con las conductas imprudentes no temerarias de sus trabajadores. Es decir, para el empresario, a mayor control, mayor conocimiento y mayor es el alcance del contenido de su obligación de seguridad. Y para el trabajador menor es su capacidad de liberalidad en el desarrollo de su actividad, es decir, una conducta imprudente no temeraria deja de serlo cuando se han adoptado todas las medidas de seguridad

necesarias, pasando a constituir entonces un incumplimiento laboral con las consecuencias jurídicas que ello conlleva desde el punto de vista de las responsabilidades.
La obtención de datos a través de estas tecnologías y su tratamiento algorítmico, siempre que se produzca dentro de los límites legales, facilitan determinar el alcance de la obligación de seguridad del empresario como garante de la salud de sus trabajadores y la conducta del trabajador como elemento exonerante o atenuante de la responsabilidad del empresario.

11. Bibliografía

AGUILAR DEL CASTILLO M.C., *El uso de la tecnología y el derecho de huelga: realidades en conflicto*, en *Labour & Law Issues*, 2018, vol. 4, n. 1, C., pp. 1-30

AGUILAR DEL CASTILLO M.C., *La protección de datos entre el contenido constitucional y su contenido legal*, en *Labour & Law Issues*, 2016, vol. 2, n. 1, I., pp. 28-43

APARICIO TOVAR J., *Los derechos fundamentales y el juicio de proporcionalidad degradados a mera retórica. A propósito de la STC 170/2013, de 17 de octubre de 2013*, en *Derecho Social*, 2013, n. 64, pp. 135-144

BARONA VILAR S., *Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?*, en *Revista Boliviana de Derecho*, 2019, n. 28, pp. 18-49

BERNARDO A., *De la tecnología wearable a la inyectable*, en *Blogthinkbig.com*, 11 junio 2015

CARDONA RUBERT M.B., *Intimidad del trabajador y comunicaciones electrónicas según el Tribunal Constitucional*, en *Lex Social*, 2015, vol. 5, n. 2, pp. 33-51

COBO DEL ROSAL M., SANCHEZ-VERA GÓMEZ-TRELLEZ J., *Responsabilidad penal por accidentes laborales*, en *Cuadernos de Política Criminal*, 2004, n. 82, pp. 5-18

DÍAZ MORENO A., MARTÍN HUERTAS M.A., *Aspectos fundamentales sobre responsabilidad y construcción en el ámbito civil*, en A. MONGE FERNÁNDEZ (dir.), *Responsabilidad y construcción. Aspectos fundamentales*, Tirant lo Blanch, 2017

GALINDO CALDÉS R., *Big data e inteligencia artificial en la gestión de los recursos humanos del sector público*, en *Revista Catalana de Dret Públic*, 2019, n. 58, pp. 49-63

GALLARDO GARCÍA R.M., *Protección jurídica de la vida y salud de los trabajadores. Derecho Penal. Derecho Administrativo sancionador*, Comares, 2016

GONZÁLEZ BIEDMA E., *Derecho a la información y consentimiento del trabajador en materia de protección de datos*, en *Temas Laborales*, 2017, n. 138, pp. 223-247

GORELLI HERNÁNDEZ J., *Responsabilidad del trabajador por incumplimiento de sus obligaciones preventivas: el caso de la construcción*, en A. MONGE FERNÁNDEZ (dir.), *Responsabilidad y construcción. Aspectos fundamentales*, Tirant lo Blanch, 2017

HILDEBRANDT M., *Esclavos de los macrodatos. ¿O no?*, en *IDP*, 2013, n. 17, pp. 7-44

IGARTUA MIRÓ M.T., *Sistema de prevención de riesgos laborales*, Tecnos, 2018

LASCURAÍN SÁNCHEZ J.A., *La prevención penal de los riesgos laborales: cinco preguntas*, en AA.VV. (coords.), *Estudios penales en homenaje al profesor Cobo del Rosal*, Dykinson, 2005

LLANEZA GONZÁLEZ P., *Seguridad y responsabilidad en la Internet de las cosas (IoT)*, Wolters Kluwer, 2018

MARTÍNEZ, Á. DE LA RÚA V., *Mi compañero de trabajo es un robot*, en *El Pais.com*, 15 noviembre 2019

MERCADER UGUINA J.R., *La robotización y el futuro del trabajo (1)*, en *Trabajo y Derecho*, 2017, n. 27, pp. 13-24

MONGE FERNÁNDEZ A., *Aspectos básicos sobre responsabilidad penal por riesgos en la construcción*, en A. MONGE FERNÁNDEZ (dir.), *Responsabilidad y construcción. Aspectos fundamentales*, Tirant lo Blanch, 2017

MORENO MUÑOZ M., *Privacidad y procesado automático de datos personales mediante aplicaciones y bots*, en *Dilemata*, 2017, n. 24, pp. 1-23

OLAIZOLA NOGALES I., *Delitos contra los derechos de los trabajadores (arts. 316 y 317 CP) y su relación con los resultados lesivos*, en *InDret*, 2010, n. 2, pp. 1-51

RODRÍGUEZ ESCANCIANO S., *Las nuevas relaciones laborales en las empresas digitales y el control empresarial*, en C. GARCÍA NOVOA, D. SANTIAGO IGLESIAS (dirs.), *4ª Revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Aranzadi, 2018

SÁNCHEZ-RODAS NAVARRO C., *Poderes directivos y nuevas tecnologías*, en *Temas Laborales*, 2017, n. 138, pp. 163-184

SÁNCHEZ-URÁN AZAÑA Y., GRAU RUIZ M.A., *El impacto de la robótica, en especial la robótica inclusiva, en el trabajo: aspectos jurídicos-laborales y fiscales*, en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2019, n. 50

SANCHO LÓPEZ M., *Internet, Big data y nuevas tecnologías: repercusiones y respuestas del ordenamiento jurídico*, en *CEFD*, 2019, n. 39, pp. 307-321

SCRIBANO A., *Drones: una manera de ver*, en *Boletín Científico Sapiens Research*, 2017, vol. 7, n. 2, pp. 65-77

VALLEJO JIMÉNEZ G.A., *Aproximación al concepto de imprudencia*, en *Nuevo Derecho*, 2010, vol. 5, n. 6, pp. 29-38

Red Internacional de ADAPT

ADAPT es una Asociación italiana sin ánimo de lucro fundada por Marco Biagi en el año 2000 para promover, desde una perspectiva internacional y comparada, estudios e investigaciones en el campo del derecho del trabajo y las relaciones laborales con el fin de fomentar una nueva forma de "hacer universidad". Estableciendo relaciones estables e intercambios entre centros de enseñanza superior, asociaciones civiles, fundaciones, instituciones, sindicatos y empresas. En colaboración con el DEAL – Centro de Estudios Internacionales y Comparados del Departamento de Economía Marco Biagi (Universidad de Módena y Reggio Emilia, Italia), ADAPT ha promovido la institución de una Escuela de Alta formación en Relaciones Laborales y de Trabajo, hoy acreditada a nivel internacional como centro de excelencia para la investigación, el estudio y la formación en el área de las relaciones laborales y el trabajo. Informaciones adicionales en el sitio *www.adapt.it*.

Para más informaciones sobre la Revista Electrónica y para presentar un artículo, envíe un correo a *redaccion@adaptinternacional.it*