FORMACIÓN PROFESIONAL Y CIBERSEGURIDAD

Sagrario Cadenas Ruiz[1]
Investigadora colaboradora de Derecho del Trabajo y de la Seguridad Social
Doctoranda en Derecho
Universidad de Santiago de Compostela

Abstract

La formación profesional continuada en ciberseguridad se ha convertido en perentoria necesidad para las personas trabajadoras y para la empresa, ante la exigencia de adaptación a un entorno cada vez más digitalizado, con indudables ventajas para la productividad y competitividad de las compañías, pero también elevados riesgos, y ello en un escenario de casi total anomia en materia de ciberseguridad. En este contexto, se reivindica el derecho de la persona trabajadora a recibir formación profesional permanente en ciberseguridad, y la apremiante necesidad para todas las empresas de disponer de un catálogo de acciones formativas para su plantilla, a fin de preservar tanto a la empresa, como a su equipo de trabajo y clientes, de los riesgos cibernéticos que se ciernen sobre cualquier organización que opera en el mercado.

Continuous professional training in cybersecurity has become a peremptory necessity for workers and for the company, given the need to adapt to an increasingly digitalised environment, with undoubted advantages for the productivity and competitiveness of companies, but also high risks, and this in a scenario of almost total anomie in cybersecurity matters. In this context, the right of workers to receive ongoing professional training in cybersecurity is demanded, and the urgent need for all companies to have a catalogue of training actions for their staff, in order to protect the company, its staff and customers from the cyber risks that loom over any organisation operating in the market.

Title: Professional training and cybersecurity

Palabras clave: Formación profesional, ciberseguridad, competencias digitales, derecho a la formación digital, aprendizaje permanente
Keywords: Vocational training, cybersecurity, digital skills, the right to digital training, lifelong learning

[1] Investigadora en formación y perfeccionamiento del Grupo de Investigación GI-1876 “Empresa y Administración”, de la Universidad de Santiago de Compostela, financiado por la Xunta de Galicia.

IUSLabor 2/2025, ISSN 1699-2938, p. 8-35
DOI. 10.31009/IUSLabor.2025.i02.01

Fecha envío: 25.2.2025 | Fecha aceptación: 9.5.2025 | Fecha publicación: 25.7.2025

Sumario

1. Introducción

La tecnología ha irrumpido en nuestras vidas como una avalancha imparable, invadiendo por completo nuestra área personal, social, y también la profesional, que es la que aquí y ahora nos ocupa. En la esfera laboral, como en todas las demás, la penetración de la tecnología ha sido tan profunda y vertiginosa que ha revolucionado la forma de trabajar en casi todos los sectores, causando una profunda transformación, entre otros aspectos, de métodos y herramientas de trabajo.

Son múltiples las ventajas que el desarrollo tecnológico proporciona a la empresa, como una mayor capacidad de respuesta rápida y ágil a las demandas de los clientes, incremento de competitividad y productividad, ahorro de tiempo y costes, o mejora de la eficiencia. Para la persona trabajadora comporta también beneficios, y uno de los más significativos es la aparición de nuevas profesiones y oportunidades de empleo. Y simultáneamente a la necesidad de hacer frente a las innovaciones tecnológicas a través de expertos que las gestionen de forma adecuada, aparecen también nuevas necesidades de capacitación y cualificación profesional que requieren de continua formación y reciclaje.
En paralelo, la tecnología tiene también consecuencias y efectos negativos, como sin duda lo son la desaparición de muchas profesiones y la pérdida de puestos de trabajo. Pero, además, en numerosos oficios y profesiones ya sucede que no es posible cumplir con la tarea encomendada a la persona trabajadora sin hacer uso de las herramientas tecnológicas, lo que en ocasiones conlleva desajustes entre las necesidades de la empresa y la cualificación de la plantilla.

Mucho se ha reflexionado sobre los conflictos que en el ámbito laboral se han planteado y se siguen planteando a causa del uso abusivo o inadecuado de las herramientas de comunicación electrónica o la navegación por internet, tanto por la persona trabajadora como por la empresa. Cuestiones como la colisión entre la facultad de control de la empresa y el derecho a la intimidad de la persona trabajadora o al secreto de sus comunicaciones (v.gr., acceso al correo electrónico) se han analizado con asiduidad tanto por la doctrina científica cuanto por los tribunales en el conocimiento de los asuntos que les competen. También han sido objeto de estudio los conflictos derivados de la transgresión de la buena fe en la utilización de los dispositivos e instrumentos tecnológicos puestos por la empresa a disposición de la persona trabajadora, ya sea por afectar a su rendimiento laboral o por ser utilizados para fines distintos del estrictamente profesional. Y, al tiempo, es asunto de continuo debate el derecho a la desconexión digital.

Sin discutir que esas materias citadas y otras similares plantean dificultades en la relación laboral que es necesario resolver, no se puede olvidar que en la actualidad cada vez cuesta más encontrar profesiones cuyas tareas se desenvuelvan sin valerse de un ordenador o

dispositivo alternativo (léase tableta, teléfono móvil o cualquier otro similar, ya inventado o que se pueda fabricar en el futuro[2]), y de una conexión a la red global. Y la experiencia demuestra que el uso habitual y continuado de la tecnología, especialmente si la ejecución del trabajo precisa de acceso a navegación por Internet, conlleva también la exposición a riesgos que pueden ser extraordinariamente amenazantes, y no solo para quien la utiliza. Más allá de la inadecuada o abusiva utilización de la tecnología por la persona trabajadora que pudiera afectar a su rendimiento laboral, se presentan otros peligros que pueden tener consecuencias perniciosas. Véase el caso de quien, en su horario laboral y haciendo uso de los dispositivos que la empresa pone a su disposición para ejecutar sus tareas, accede a páginas pornográficas. Es el supuesto enjuiciado por el Tribunal Superior de Justicia del Principado de Asturias, que declaró procedente el despido de un trabajador por entender que, al acceder a páginas de contenido erótico y pornográfico durante su jornada laboral y utilizando los medios materiales de la empresa para sus fines particulares, no solo estaba incurriendo reiterada y conscientemente en una conducta expresamente prohibida por la empresa (constando probado en autos su conocimiento de la prohibición), sino que además consideró el Tribunal que la conducta constituía "*una grave y culpable responsabilidad por imprudencia en acto de trabajo, al existir peligro cierto y conocido por cualquier usuario de internet de afectación del sistema informático en red de la empresa por virus al acceder a páginas web de contenido erótico y pornográfico por tratarse de páginas de alto riesgo en este sentido*" [3].

Se trata, quizá, de un caso extremo, en el que el Tribunal estimó que era un hecho notorio el alto riesgo que presentan los accesos a páginas con este tipo de contenido. Pero otros muchos no son tan evidentes. Como muestra podemos citar la posibilidad de facilitar a los ciberdelincuentes el acceso a información confidencial de la empresa, mediante actos intencionados, maliciosos o negligentes de la persona trabajadora, o incluso sin voluntariedad alguna, simplemente por desconocimiento, ignorancia o exceso de confianza. El Tribunal Superior de Justicia de Valencia[4] calificó como procedente el despido de un trabajador por considerar que había incurrido en una negligencia inexcusable, pese a no constar una conducta dolosa ni intencionada, al servir de vehículo para que su empresa fuese víctima de un fraude realizado a través de la técnica

[2] El Instituto Nacional de Ciberseguridad de España (INCIBE) habla, de forma genérica, de "*dispositivos conectados* [sic]*, tales como teléfonos móviles, drones o sistemas de control industrial*". Se trata, por tanto, no solo de la vulnerabilidad de terminales de comunicación, sino también de herramientas de control y funcionamiento de instalaciones públicas y privadas, e incluso de infraestructuras críticas. Disponible en: https://www.incibe.es/empresas/blog/la-comision-europea-presenta-una-nueva-propuesta-de-resiliencia-cibernetica; consulta: 17.10.2024.

[3] STSJ Principado de Asturias, Sala de lo Social, n.º 2238/2010 de 30 de julio (rec. n.º 1669/2010)

[4] STSJ Valencia, Sala de lo Social, n.º 3497/2021 de 30 de noviembre (rec. n.º 2239/2021).

denominada *phishing*[5]. Para decretar la procedencia del despido, el Tribunal tuvo muy en cuenta las medidas preventivas adoptadas por la empresa para defenderse de posibles fraudes informáticos, destacando que disponía de herramientas tecnológicas de ciberseguridad en sus equipos y de una normativa específica de seguridad de la información actualizada de forma periódica que se notificaba a cada miembro del equipo de trabajo; que se llevó a cabo una campaña de sensibilización de los integrantes de la plantilla para alertarles de posibles fraudes (*phishing*); y que disponía también de un plan de formación y de cursos en protección de datos y en cumplimiento de rúbricas en el ámbito penal (*compliance)* para todo el personal.

Similar manifestación de un riesgo de seguridad informática es la técnica denominada *ransomware*, que el Instituto Nacional de Ciberseguridad de España (INCIBE) define como "*tipo de «malware»* [sic] *que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo*"[6]. Según explica el mencionado Instituto, la infección de los equipos se produce a través de diversos métodos, entre los que destaca el envío de correos electrónicos a las víctimas para que descarguen archivos adjuntos o accedan a sitios web maliciosos, o la introducción en los equipos corporativos de dispositivos externos infectados, entre otros.

Conviene resaltar estos concretos supuestos precisamente porque quizá sean los más idóneos, y también los más habituales, para que una persona trabajadora sin la suficiente preparación en materia de ciberseguridad se convierta en víctima propiciatoria que facilite un ataque informático a la empresa y posibilite el secuestro de datos y la extorsión.

En los casos mencionados el defraudador habitualmente persigue un beneficio económico mediante la obtención de un desplazamiento de fondos de la empresa, pero este tipo de técnicas pueden tener otros objetivos distintos del directamente pecuniario, como la apropiación indebida de información valiosa de la compañía o de datos confidenciales de sus clientes y usuarios, o incluso de los propios miembros del personal[7] (identidades, domicilios o cuentas bancarias, entre otros).

---

[5] El INCIBE define el *phishing* como *"una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico"*. El mismo objetivo e idéntica estrategia de simulación tienen otras técnicas que utilizan el teléfono (*vishing)*, o el SMS (*smishing)*. Disponible en: https://www.incibe.es/aprendeciberseguridad; consulta: 17.10.2024.

[6] Disponible en: https://www.incibe.es/aprendeciberseguridad/ransomware; consulta: 17.10.2024.

[7] Clientes y personas empleadas suelen ser los más afectados por violaciones de seguridad en las empresas, siendo sus datos personales y financieros una información especialmente valiosa para los ciberdelincuentes.

Tratándose de secretos empresariales[8], la comisión por cualquier integrante de la plantilla de una conducta dolosa, imprudente o negligente, que facilite su robo por terceros, puede causar un grave daño patrimonial a la empresa. Pero si hablamos de apropiación de información de carácter personal de personas físicas, objeto de protección cualificada por afectar a un derecho fundamental[9], podemos fácilmente concluir que quien divulgue, revele o publique datos personales de clientes o del personal de la organización, sin causa y sin conocimiento ni consentimiento de los afectados, puede acarrear la responsabilidad de la empresa por daños causados a terceros por sus dependientes[10].

El daño para la empresa, ya sea en los mencionados supuestos de infracciones o violaciones de seguridad en materia de protección de datos, ya por cualquier otro motivo sucedido en el ciberespacio y del que sea autor (o vehículo facilitador) un integrante de la compañía, puede ser patrimonial, pero es más que probable que sea por añadidura reputacional, pues no cabe duda de que un incidente grave de seguridad informática irá en detrimento de la imagen de marca de una entidad, con la consiguiente pérdida de confianza en el mercado.

Ahora bien, no solo cabe contemplar la responsabilidad civil de la empresa por daños patrimoniales causados por sus dependientes, o la pérdida de prestigio por las actuaciones de estos. A la vez, es posible la apreciación de responsabilidad penal, ya que el artículo 31 bis del vigente Código Penal (CP)[11] determina las circunstancias en las que la persona jurídica será penalmente responsable de los delitos cometidos en su nombre o por su cuenta, y en su beneficio directo o indirecto, por sus representantes legales, integrantes

---

Sobre esta cuestión, véase MUÑOZ RUIZ, Ana Belén, "Cómo afecta la ciberseguridad a los derechos laborales de las personas empleadas y sindicatos. Comentario a la Sentencia del Tribunal Supremo 1033/2020, de 25 de noviembre", *Revista de Trabajo y Seguridad Social,* n.º 459, 2021, p. 211-212.

[8] Definidos por el artículo 1 de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales como *"cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto."*

[9] La protección de las personas físicas en relación con el tratamiento de datos personales tiene la consideración de derecho fundamental. Artículo 18.4 de la Constitución Española, Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los derechos digitales, y 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).

[10] Artículo 1903 del Código Civil, en relación con el 1902.

[11] Introducido por la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

de sus órganos de decisión o personas sometidas a la autoridad de estos. Conforme a este precepto, los delitos cometidos por las personas trabajadoras en el ejercicio de su labor y en el ámbito digital pueden igualmente acarrear la responsabilidad penal de la empresa, con severas sanciones[12] que incluso podrían suponer la disolución de la persona jurídica en los casos más cualificados.

Llegados a este punto, es obligado aludir a las consecuencias que este tipo de situaciones pueden conllevar para la persona empleada que resulte ser la última responsable de los actos que, voluntaria o involuntariamente, hayan ocasionado o sean susceptibles de ocasionar perjuicios a su empresa o a terceros[13]. Obviamente la sanción disciplinaria dependerá en cada caso de la gravedad de los hechos cometidos y de las circunstancias concurrentes, mas es innegable que la conservación del propio puesto de trabajo puede depender en gran medida de la instrucción previa que la persona trabajadora haya recibido sobre los riesgos cibernéticos y su evitación. Sin duda no se puede valorar igual la conducta dolosa o negligente de una persona adecuadamente entrenada para reconocer los riesgos cibernéticos y defenderse de ellos, que la de aquella carente de la formación e información oportuna sobre el particular.[14]

De lo anterior se deduce, por tanto, que el correlativo riesgo para la empresa es la posible calificación de improcedencia[15] de las sanciones disciplinarias aplicadas sin previa adopción de medidas preventivas para evitar, paliar o mitigar la facilitación de ataques informáticos por los integrantes de la plantilla, ya sea conscientemente o sin intención dolosa. Si algo se desprende con claridad de las sentencias más arriba citadas, dictadas en materia de despido por causas vinculadas a la ciberseguridad, es la valoración por los Tribunales de la previa y adecuada instrucción de la persona trabajadora en esta materia.

---

[12] Calificadas todas ellas de graves por el artículo 33.7 del CP.

[13] Viene al caso recordar que la doctrina jurisprudencial consolidada valora como sancionable la transgresión de la buena fe contractual por la persona trabajadora aun cuando no se haya producido un daño real. Véase STS, Sala Cuarta, de lo Social, de 19.07.2010 (rec. n.º 2643/2009): *"La inexistencia de perjuicios para la empresa o la escasa importancia de los derivados de la conducta reprochable del trabajador, por una parte o, por otra parte, la no acreditación de la existencia de un lucro personal para el trabajador, no tiene trascendencia para justificar por sí solos o aisladamente la actuación no ética de quien comete la infracción, pues basta para tal calificación el quebrantamiento de los deberes de buena fe, fidelidad y lealtad implícitos en toda relación laboral"*.

[14] *"El principal problema que presenta la presencia de las nuevas tecnologías en las relaciones laborales es la capacidad que tienen de constituir motivo legal de despido objetivo o despido disciplinario, por la falta de destreza en su uso o por el mal uso que, de las mismas, puede llegar a hacer el empleado"*. BALLESTER CASANELLA, Blanca, "Los nuevos desafíos que plantean las nuevas tecnologías en el ámbito de la desvinculación laboral", *Revista de Derecho, Empresa y Sociedad (REDS),* n.º 22-23, 2023, p. 44. (disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9294271; consulta: 22.10.2024).

[15] Incluso nulidad, en caso de concurrir discriminación o violación de derechos fundamentales o libertades públicas de la persona trabajadora.

A sensu contrario, la falta de diligencia de la empresa en la adopción de mecanismos precautorios apropiados y suficientes para prevenir riesgos informáticos tendrá un importante peso en la consideración como improcedente de un eventual despido por actos indebidos o imprudentes de la persona trabajadora que no ha sido adecuadamente adiestrada.

De seguir reflexionando sobre potenciales peligros, con toda seguridad podríamos engrosar esta lista con más amenazas. El problema es que siempre habrá quien dedique su tiempo y sus esfuerzos a inventar nuevas fórmulas de ataque informático para aprovechar las debilidades de particulares, Estados o empresas, con el fin de sacar provecho de ellas. Y dado que el mundo digital es el camino por el que forzosamente van a transitar, el insoslayable recurso de las compañías es protegerse y proteger a su equipo de trabajo.

En este contexto, es obvio que la primera barrera de protección que se adopta por las empresas como potenciales víctimas de posibles ataques informáticos es el reforzamiento de medidas técnicas de ciberseguridad, y no cabe duda de que así ha de ser. Disponer de instrumentos tecnológicos modernos, efectivos y actualizados para prevenir y repeler ataques informáticos, así como de personal cualificado que las gestione, es innegablemente el muro de contención básico del que no conviene prescindir.

Sin embargo, la ciberseguridad tiene otra vertiente igualmente importante: no es una tarea que competa solo a los técnicos especializados en proteger a las compañías, personas y Estados de los peligros que les acechan en la realidad virtual, sino también a todos y cada uno de los agentes que desempeñan su diaria labor en las empresas, ya sean pymes o grandes organizaciones, y que solo por hacer uso de las nuevas tecnologías se exponen de igual modo a sus riesgos. Siendo trascendental la necesidad de capacitar a profesionales especialmente cualificados en materia de ciberseguridad para que desarrollen adecuadamente la labor para la que fueron contratados, y siendo también imprescindible que estos profesionales reciban continuo reciclaje y recualificación para hacer frente desde el punto de vista técnico a innovaciones tecnológicas que impliquen nuevas ciber amenazas, es asimismo vital concienciar y formar al personal no especializado, que es altamente vulnerable y susceptible de ser objeto de aquellas y de poner en peligro a toda una organización.

Ha de tenerse en cuenta que puede tratarse de actos dolosos de las personas trabajadoras, o sea, voluntarios, intencionados y maliciosos, o culposos en el sentido de imprudentes, incluida la imprudencia profesional, pero también de actuaciones inconscientes, ocasionadas por ignorancia o desconocimiento o, simplemente, negligentes.

Y, si la necesidad de formación e información en este ámbito se incrementa en la etapa de madurez para hacer frente a las carencias de la persona trabajadora por falta de previa preparación en competencias digitales, no es menos relevante en la horquilla de menor edad, como lo demuestra la incidencia de afectación de los delitos cibernéticos en esta franja[16].

Ante este elenco de eventuales contingencias, que no parece que vayan a disminuir con el progreso tecnológico, sino que más bien apuntan a incrementarse y a evolucionar hacia peligros cada vez más sofisticados, es obligado analizar la regulación de la ciberseguridad en el ámbito laboral, tanto en la ley como en los convenios colectivos y, a su vista, el alcance y dimensión del derecho de las personas trabajadoras a la formación en esta materia.

2. La ciberseguridad en la legislación laboral: la incipiente aportación de la negociación colectiva

La ciberseguridad afecta a todos los ámbitos de la sociedad y, por ende, a la esfera del Derecho del Trabajo. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) la considera *"la piedra angular de la transformación digital"* y la señala como necesidad *"transversal a todos los sectores"*[17]. Y la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, la califica como uno de los ámbitos de especial interés para la seguridad nacional[18].

El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»), define la ciberseguridad en su artículo 2 como *"todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas"*[19].

---

[16] Informe sobre cibercriminalidad en España 2023 (Ministerio del Interior). Disponible en: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf; consulta: 16.01.2025.

[17] Disponible en: https://www.enisa.europa.eu/about-enisa/about/es; consulta: 21.10.2014.

[18] Definidos por la propia Ley de Seguridad Nacional en su artículo 10 como *"aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales"*.

[19] A esta definición se remite también en su artículo 6.3 la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Si atendemos al último inciso de la definición, es claro que en el terreno de la relación laboral pueden verse afectados por incidentes de seguridad informática tanto la propia empresa como sus clientes, usuarios y personas empleadas. Y estas últimas, además de potenciales víctimas, pueden convertirse en agentes que, sea de forma activa o por inacción, propicien aquellos incidentes. Mas a pesar del incremento del riesgo de ataques a causa de la cada vez más elevada dependencia tecnológica de las compañías, no es esta una materia que esté contemplada de forma expresa en la regulación positiva, más allá de cuestiones puntuales como la protección de datos de carácter personal[20] o, ya en el específico ámbito de las relaciones laborales, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral[21], el derecho a la desconexión digital[22] o el teletrabajo[23].

Ahora bien, pese a la conciencia generalizada y consolidada en todos los ámbitos de que la alta dependencia de la tecnología y la interconexión de los sistemas de información sitúan a todos los sectores en continuo escenario de riesgo, la legislación laboral no ha dado aún respuesta a las contingencias a las que se ven expuestas empresas y personas trabajadoras por eventuales ataques informáticos.

Lo cierto es que las empresas precisan que los componentes de su plantilla dominen las tecnologías para poder hacer uso de ellas, lo que conlleva una inherente necesidad de que, en la misma medida, conozcan y entiendan sus posibles efectos y consecuencias para evitar, prevenir y mitigar sus riesgos. Dicho de otra forma, todos los integrantes de una organización, desde los órganos de dirección hasta el personal de cualquier nivel, sea cualificado o no especializado, y que se encuentren en situación de ser víctima o vehículo facilitador de un ataque informático, han de tener el deber y, por tanto, el correlativo derecho de estar permanentemente formados e informados en materia de ciberseguridad, a la vista de la posibilidad cierta de poner en riesgo cuestiones tan trascendentes como el patrimonio, la reputación y la información sensible de la compañía y de terceros o la suya propia y, por ende, su puesto de trabajo.

---

[20] 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), y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD), ambos aplicables *"al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"*.

[21] Artículo 20 bis del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET) y artículo 87 de la LOPDPGDD.

[22] Artículo 88 de la LOPDPGDD.

[23] Artículos 17, 18, 20 y 21 de la Ley 10/2021, de 9 de julio, de trabajo a distancia.

Sin embargo, pese a la trascendencia de las cuestiones de seguridad informática en el terreno de las relaciones laborales, el legislador social no ha abordado aún las transformaciones introducidas por la tecnología. En este contexto de anomia adquiere especial relevancia la negociación colectiva[24], y aunque en este ámbito sí se aprecia mayor atención a las cuestiones de ciberseguridad en la relación laboral, tampoco encontramos una respuesta suficiente y adecuada, más allá de las continuas prevenciones sobre la facultad sancionadora de la empresa por infracciones cometidas por su personal en materia de seguridad informática.

Ello no solo implica que se hace hincapié en la responsabilidad de la persona trabajadora y no en la de la empresa, sino que además pone de manifiesto que se está obviando la trascendental cuestión de la prevención, aspecto que es tanto o más importante que la medida reactiva sancionatoria cuando ya se ha producido un incumplimiento. La pregunta es: ¿Resulta prioritario evitar el incidente informático o lo es sancionar al responsable cuando aquel ya se ha producido y el perjuicio se ha ocasionado? La respuesta parece más que obvia: Si se emplea el esfuerzo en que el ataque no prospere, se evitará, o al menos se paliará, su efecto pernicioso sobre el patrimonio, la reputación o la información sensible de las organizaciones y sus integrantes. Y además téngase en cuenta que una actuación culposa o dolosa de la persona trabajadora ni siquiera tendría por qué estar expresamente prevista en el contrato de trabajo o en el convenio para ser sancionada.

Con todo, tampoco son demasiados los convenios colectivos que prevean con detalle las vicisitudes propiciadas por el uso de la tecnología con relación a la seguridad informática, ni siquiera en sectores particularmente expuestos a riesgos cibernéticos[25] o relacionados de forma directa con áreas específicamente tecnológicas[26]. Aunque en realidad, no es este el elemento que deba determinar la necesidad de acometer esta materia. A priori podríamos incurrir en el pensamiento prejuicioso de que solo las empresas incluidas en las mencionadas categorías necesitan disponer de una política específica de ciberseguridad. Sin embargo, es más que evidente que la clave se encuentra en la utilización de herramientas tecnológicas y dispositivos conectados como instrumento de trabajo o como sistema de comunicación, gestión y manejo de información. Este es, en realidad, el verdadero factor que determina la exposición al riesgo. Desde esta perspectiva, cualquier compañía, sea gran empresa o pyme, puede ser blanco de ataques

[24] Significativamente si se atiende a la remisión (sin carácter de obligatoriedad) que el artículo 91 de la LOPDPGDD hace a la negociación colectiva en relación con *"la salvaguarda de derechos digitales en el ámbito laboral"*.

[25] Léase, *verbi gratia*, las empresas del sector financiero que manejan elevadas cantidades de fondos propios y ajenos y que son blanco favorito de ciberdelincuentes que persiguen desplazamiento de dinero fácil y rápido.

[26] Tecnologías de la información, consultoría tecnológica, servicios de informática y afines.

a causa de la informatización o digitalización de sus sistemas, y hoy por hoy es difícil encontrar una que esté exenta de sufrirlos. El INCIBE advierte que no podemos dejarnos llevar por la falsa creencia de que las pequeñas y medianas empresas no son objetivo de la ciberdelincuencia. Bien al contrario, estas últimas acumulan valiosa información (datos personales y/o bancarios, contraseñas, documentos de identidad) y además pueden servir de puente para acceder a organizaciones más grandes[27].

Sin ánimo exhaustivo, podemos comenzar por destacar el Convenio colectivo de Iberdrola Grupo[28], que, además de establecer las normas de utilización de los recursos y medios informáticos puestos a disposición de su personal, utiliza el término exacto de ciberseguridad y determina su concepto a efectos del convenio[29].

Otros convenios aluden a la seguridad informática sin hacer uso del término ciberseguridad y, con mayor o menor grado de exhaustividad, regulan las normas de uso y prevén supuestos de utilización abusiva de las herramientas informáticas y digitales. Es el caso del Convenio colectivo marco del Grupo Endesa[30], que en su artículo 130 se remite al régimen disciplinario en caso de incumplimiento de la política de uso de las nuevas tecnologías de la información.

En los mismos términos, y con igual o incluso mayor detalle, el Convenio colectivo de Telefónica de España, SAU; Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones, SAU[31], regula en su artículo 168 la utilización de

[27] Disponible en: https://www.incibe.es/index.php/empresas/blog/datos-robados-descubre-que-hacen-los-ciberdelincuentes-con-ellos-y-como-protegerte; consulta: 2.12.2014.

[28] Resolución de 18 de febrero de 2021, de la Dirección General de Trabajo, por la que se registra y publica el VIII Convenio colectivo de Iberdrola Grupo. «BOE» n.º 52, de 2 de marzo de 2021, p. 24833-24930.

[29] La define en su artículo 90: *"Se entiende por ciberseguridad las tecnologías, procesos y las buenas prácticas diseñados para proteger la infraestructura frente a ataques, daños o accesos no autorizados. Se entiende por ciberinfraestructura el conjunto de servicios de información y comunicaciones electrónicas, así como la información contenida en los mismos. Estos conceptos abarcan tanto al hardware como al software para procesar, almacenar, enviar información o cualquier combinación entre estos elementos, y hace referencia a los sistemas informáticos y de comunicación, a los sistemas de control y supervisión de las operaciones de generación, transporte y distribución de energía, a las redes internas y externas y a los servicios y herramientas de seguridad."*

[30] Resolución de 4 de junio de 2020, de la Dirección General de Trabajo, por la que se registra y publica el V Convenio colectivo marco del Grupo Endesa. «BOE» n.º 169, de 17 de junio de 2020, p. 41350-41456.

[31] Resolución de 16 de febrero de 2024, de la Dirección General de Trabajo, por la que se registra y publica el III Convenio colectivo de Telefónica de España, SAU; Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones, SAU. «BOE» n.º 52, de 28 de febrero de 2024, p. 23855-24058.

dispositivos digitales corporativos, software y aplicativos, correo electrónico, sistema de mensajería y herramientas sociales y colaborativas y el acceso a internet, estableciendo:

> *"Las directrices necesarias y las acciones de control y corrección adecuadas sobre la buena utilización de las nuevas tecnologías por parte de las personas trabajadoras, con el fin de prevenir las prácticas abusivas sobre una utilización particular de los medios informáticos que se pudieran producir, y sobre todo de aquéllas que puedan poner en riesgo la seguridad de los sistemas informáticos".*

Véase que esta afirmación, aun sin poner negro sobre blanco el término ciberseguridad, sí habla directamente de riesgo cibernético a causa de la utilización indebida de la tecnología. Y, en la misma línea que el anterior y otros similares, prevé la aplicación del oportuno régimen disciplinario en caso de incumplimiento de las normas de utilización de las herramientas y sistemas informáticos, así como un procedimiento de comprobación por la empresa ante sospechas de uso ilícito o abusivo.

En lo que concierne al asunto que aquí nos ocupa, es de destacar que el citado convenio del grupo Telefónica dedica su Capítulo VIII a la *"Formación"*, que califica como *"valor estratégico que permite la adaptación de la Empresa y de las personas trabajadoras a las nuevas tecnologías y a las necesidades del mercado"*, estableciendo como obligatorias las acciones formativas que se requieran en cada momento para las necesidades de capacitación de la plantilla. E igualmente relevante es el hecho de que su artículo 40 subraya que la formación es *"un proceso permanente"* y que marca como objetivo, entre otros, un *"reciclaje que permita la mayor y más rápida adaptación de la plantilla a los requerimientos de las nuevas funcionalidades o avances tecnológicos"*. En cuanto que es una alusión amplia, cabe imaginar que entre estos requerimientos se incluye la capacitación de su plantilla en materia de ciberseguridad.

En suma, el tratamiento convencional de la seguridad informática incide prioritariamente en las obligaciones de las personas trabajadoras referidas a la ejecución de la prestación de servicios cuando utilizan para ello instrumentos tecnológicos, y en las consiguientes sanciones por su incumplimiento, pero hay una casi total ausencia de referencia a las obligaciones preventivas de la empresa y a la necesidad perentoria de dotar al personal de herramientas que le proporcionen una sólida cultura de ciberseguridad y que le permitan hacer frente a eventuales peligros cibernéticos.

Ciertamente, en la práctica judicial la diligencia exigible a la persona empleada dependerá en gran medida de la que correlativamente haya adoptado su empresa para entrenarle frente a los riesgos, lo que, a falta de legislación expresa, conduce a reivindicar un papel reforzado de la negociación colectiva en materia de ciberseguridad en la relación laboral,

y un mayor compromiso de los agentes sociales con la protección de las personas trabajadoras en el entorno digital[32].

Con la vista puesta en esta tesitura, la negociación colectiva ha de tomar conciencia de la vital trascendencia de los riesgos de la tecnología en la relación de trabajo. Si sus predecesores ya reconocían la necesidad de insertar como objetivo fundamental en los convenios colectivos la *"incidencia de las tecnologías de la información y de la comunicación en el desarrollo productivo general y en las relaciones laborales*"[33], el V Acuerdo para el Empleo y la Negociación Colectiva (V AENC)[34] señala la ruta a seguir cuando propugna *"la adaptación permanente de las plantillas a las nuevas realidades a las que se enfrenta el mundo del trabajo"*, para cuyo objetivo considera *"imprescindibles los planes de formación permanente que, con las necesarias actualizaciones, capaciten a las trabajadoras y trabajadores para responder a esas nuevas realidades, marcadas, entre otras, por la transición digital…"*.

Sobre la base de la necesidad de hacer frente a las profundas transformaciones digitales que la sociedad y el mercado de trabajo demandan, el V AENC aborda cuestiones determinantes como la trascendencia de la formación continua, permanente y constante en la transición digital de empresas y personas trabajadoras[35], o la conveniencia de que

---

[32] *"El papel de los representantes de los trabajadores y la negociación colectiva es fundamental en la implantación de nuevas tecnologías y la protección frente a la ciberseguridad en el entorno laboral."* Estas son las palabras recogidas en el informe AA. VV., *Guardianes digitales para un crecimiento sostenible: Ciberseguridad y protección ciudadana en la era de la transformación digital,* VAQUERO GARCÍA, Alberto. (director), Madrid, Consejo Económico y Social de España, 2024, p. 189, que inciden en la afirmación recogida *supra*. El informe, en alusión a la situación de las pymes, compañías que por su menor tamaño tienen mayor dificultad para contar con un convenio colectivo propio que contemple sus necesidades y singularidades, propone la solución de los convenios provinciales como *"alternativa más cercana a su realidad socioeconómica"*, si bien, por tratarse de convenios que no suelen abordar los *"cambios tecnológicos más avanzados de nuestra sociedad"*, será primordial actualizarlos *"para asegurar que las PYMES* [sic] *puedan adaptarse y sobrevivir en un entorno cada vez más digitalizado"*. *Ibidem,* p. 191.

[33] Resolución de 15 de junio de 2015, de la Dirección General de Empleo, por la que se registra y publica el III Acuerdo para el Empleo y la Negociación Colectiva 2015, 2016 y 2017, Capítulo II. «BOE» núm. 147, de 20 de junio de 2015, p. 51602 a 51619.

[34] Resolución de 19 de mayo de 2023, de la Dirección General de Trabajo, por la que se registra y publica el V Acuerdo para el Empleo y la Negociación Colectiva. «BOE» núm. 129, de 31 de mayo de 2023, p. 75426 a 75447.

[35] V AENC, Capítulo V: Formación y cualificación profesional. En este aspecto, el Acuerdo se alinea con el objetivo de *"formación continua de nuestra mano de obra actual y futura y de las empresas con las aptitudes adecuadas para aprovechar las oportunidades y hacer frente a los retos de la transformación digital en el mundo laboral"* que inspira el Acuerdo Marco Europeo sobre Digitalización, suscrito por los interlocutores sociales europeos (disponible en idioma español en: https://www.ceoe.es/es/publicaciones/laboral/acuerdo-marco-de-los-interlocutores-sociales-europeos-sobre-digitalizacion; consulta: 14/05/2025).

los convenios colectivos incluyan *"programas de formación e información sobre los riesgos del uso de las nuevas tecnologías del trabajo y las medidas preventivas a adoptar frente a los mismos, además de criterios de buenas prácticas respecto a la digitalización"*[36], siendo especialmente relevante el hecho de que este último objetivo se inserte en el epígrafe destinado a la mejora de las condiciones de seguridad y salud en el trabajo. Esta última cuestión no hace más que incidir en la ya señalada perentoriedad de proyectar programas formativos, de forma periódica y mantenida, para la capacitación constante de los equipos de trabajo frente a los riesgos cibernéticos.

3. El alcance del derecho de la persona trabajadora a recibir formación e información constante en materia de ciberseguridad

La ENISA califica la ciberseguridad como *"responsabilidad compartida"* y pone el acento en la necesidad de capacitación: *"La frecuencia y la sofisticación de los ciberataques aumenta a gran velocidad, al tiempo que las personas, las organizaciones y las industrias hacen cada vez mayor uso de las tecnologías e infraestructuras de TIC. Las necesidades de competencias y conocimientos en materia de ciberseguridad son mayores que la oferta. La UE tiene que invertir en crear competencias y talentos en ciberseguridad a todos los niveles, desde el personal no especializado hasta el profesional altamente cualificado"*[37].

En la misma línea y con similar contundencia se expresa el INCIBE: *"El usuario es el eslabón más IMPORTANTE* [sic] *de la cadena de la seguridad"*[38]. Incide este Instituto en la idea de que las tecnologías, procesos y herramientas más avanzadas y sofisticadas creadas para defenderse de ataques informáticos no serán nunca suficientes si las personas trabajadoras no observan un mínimo de buenas prácticas. Y como no puede ser de otra forma, para conseguir este objetivo recomienda una política empresarial con dos líneas intrínsecamente unidas: Formación y concienciación del equipo humano de trabajo.

La sensibilización y concienciación de las personas trabajadoras sobre la importancia de la seguridad informática es fundamental para que la enfrenten con la responsabilidad y prudencia que merece, y la asuman como propia y conveniente en lugar de entenderla como un requerimiento caprichoso de la empresa. Entender las pautas y las instrucciones que se imparten a la plantilla sobre ciberseguridad, a la par que -y especialmente- sus motivos, es esencial para ponerlas en práctica. Pero para ello se requiere la implantación de un proceso formativo adecuado a las circunstancias de cada organización. Y en lo que

[36] V AENC, Capítulo VIII: Seguridad y salud en el trabajo.

[37] Disponible en: https://www.enisa.europa.eu/about-enisa/about/es; consulta: 21.10.2014.

[38] Disponible en: https://www.incibe.es/empresas/que-te-interesa/desarrollar-cultura-en-seguridad; consulta: 25.10.2024.

atañe a la formación, el INCIBE subraya, entre otros, los siguientes aspectos: 1) debe ser continuada en el tiempo; 2) su grado debe ajustarse al nivel de cada puesto de trabajo y a las necesidades de cada sector; y 3) ha de abarcar tanto los aspectos técnicos como los organizativos y legales en pro de una mayor seguridad, con miras a la protección de la información, patrimonio y reputación de la propia empresa, y, desde luego, a la evitación de la comisión de infracciones legales (v.gr., situaciones ya aludidas sobre protección de datos, o responsabilidad civil o penal, entre otras)[39].

La gran mayoría de personas empleadas trabaja con dispositivos conectados, por lo que todos ellos, y no solo el personal específicamente informático, necesitan la oportuna formación de ciberseguridad. Sin embargo, la exigencia no puede ser la misma para los técnicos especialistas que para los usuarios finales, y mientras los informáticos requerirán una formación constante sobre avances tecnológicos, otros puestos deberán ser especialmente entrenados en riesgos relacionados con la seguridad de la información, o con peligros de infección por virus o de estafas. En cambio, lo que sí comparten todos los niveles de la organización es la necesidad de que la formación sea continua y permanente.

Nos encontramos en un entorno de acelerado desarrollo de la tecnología, lo que redunda en una obsolescencia muy rápida de la formación en materia de seguridad informática. Esa *"constante innovación tecnológica hace que queden rápidamente desfasadas las soluciones normativas adoptadas en las empresas con vistas al reciclaje del personal a corto plazo"*[40]. Aun refiriéndose esta afirmación a la obsolescencia profesional de personas de edad madura y situación de paro prolongado, no deja de ser un aserto plenamente aplicable a las capacidades y habilidades digitales de las personas trabajadoras de todo segmento de edad, que van a necesitar constante entrenamiento para hacer frente a las amenazas cibernéticas, habida cuenta de que las técnicas de los ciberdelincuentes evolucionan y se renuevan constantemente para sortear la resistencia de sus potenciales víctimas.

En términos de utilidad, la formación, para ser efectiva, *"debe ser relevante, práctica y, lo más importante, continua"*[41]. De ahí que la doctrina respalde la responsabilidad de las

[39] Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf; consulta: 25.10.2024.

[40] DE CASTRO MEJUTO, Luis Fernando, "La formación profesional de los trabajadores de edad madura frente a la brecha digital", en MELLA MÉNDEZ, Lourdes (directora) y FERREIRO REGUEIRO, Consuelo (coordinadora), *La formación profesional para la empresa y la sociedad del siglo XXI: Puntos críticos,* Cizur Menor (Navarra), Aranzadi, 2023, p. 324.

[41] AA. VV., *Guardianes digitales para un crecimiento sostenible: Ciberseguridad y protección ciudadana en la era de la transformación digital, ob. cit.,* p. 179. Esta publicación, producto de una profunda investigación sobre la ciberseguridad y su impacto socioeconómico desde diversas perspectivas (social,

empresas como suministradoras de formación específicamente en materia de ciberseguridad, abogando por la implantación de programas formativos coherentes, y por una formación *"continua, adaptada y adaptable"* que permita a la persona empleada encarar los cambios tecnológicos que se introduzcan por la empresa en el proceso de producción[42].

Por otro lado, es oportuno mencionar que, en numerosas ocasiones, las infracciones de seguridad informática de las personas trabajadoras ni siquiera tienen carácter intencionado, doloso o imprudente (por ejemplo, la no adopción medidas básicas de protección ante posibles ataques), tratándose en otros muchos casos de meras acciones involuntarias que obedecen al desconocimiento o que resultan negligentes por el descuido o la creencia ignorante de no estar cometiendo falta alguna.

Este escenario conduce directamente a la reflexión que subyace en la base del presente trabajo. Si la legislación laboral es prácticamente inexistente en materia de ciberseguridad, y si atendemos a la consideración generalizada que comparten los (no demasiados) convenios colectivos que sí tratan la materia, en el sentido de que es obligación de la persona trabajadora cumplir las medidas básicas de protección y seguridad informática que establezca la empresa (so pena de imposición de sanciones, a veces tan graves como el despido), la única conclusión razonable es que también en materia de ciberseguridad resulte imperioso preconizar un derecho de los integrantes de la plantilla a recibir formación profesional a cargo de la empresa, de igual forma que tienen reconocido este derecho en relación con otras habilidades y competencias digitales que precisen para desarrollar adecuadamente sus funciones.

El mencionado derecho a la capacitación de la persona trabajadora para lograr su adaptación a las modificaciones técnicas operadas en su puesto de trabajo se desprende de forma expresa de la legislación positiva, por cuanto el artículo 52 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET), determina que *"el empresario deberá ofrecer al trabajador un curso dirigido a facilitar la adaptación a las modificaciones operadas"*. La doctrina ha considerado que esta norma representa la *"tutela jurídica de las aspiraciones empresariales en materia de innovación y aumento de la competitividad"*, a la vez que encarna un *"importante auge del derecho a la formación del trabajador"*, y

económica o laboral, entre otras), subraya que la ciberseguridad *"no es un estado que se alcanza y se mantiene estático; es un proceso dinámico que requiere una adaptación y aprendizaje constantes."*

[42] ÁLVAREZ CUESTA, Henar, "La ciberseguridad en la empresa: Una aproximación desde el derecho del trabajo", *Derecho de las relaciones laborales*, n.º 7, 2019, p. 689-690.

es un *"síntoma más de un florecimiento del derecho a la formación como principal abrigo de la parte trabajadora, y su intrínseca debilidad, dentro del mercado de trabajo"*[43].

Sin perjuicio del carácter razonable que la norma exige que deben revestir las modificaciones, lo cierto es que los Tribunales han considerado de forma sostenida, casi desde el inicio de la digitalización de las organizaciones, que el empleo de la informática en los procesos productivos no solo se justifica, sino que conviene y se necesita[44]. Interés empresarial, por otra parte, *"de todo punto fundado, puesto que la empresa que descuide su adaptación al devenir tecnológico arriesga su propia supervivencia"*[45].

Tanto el derecho de la persona trabajadora a recibir la formación como el correlativo deber empresarial de suministrarla que se derivan de la circunstancia prevista en el artículo 52.b ET, se consideran por la doctrina coherentes con el derecho que en la relación de trabajo reconoce el artículo 4.2.b) ET a los trabajadores a la *"promoción y formación profesional en el trabajo, incluida la dirigida a su adaptación a las modificaciones operadas en el puesto de trabajo"*, puesto que el actual carácter obligatorio de la formación *"conecta sin dificultad con el contenido del derecho a la formación del trabajador que ahora luce el artículo 4.2.b) ET"*[46]. Así, la extinción del contrato por esta causa se justifica *"por una parte, en el derecho del empresario a la innovación tecnológica en los procesos productivos y, por otra parte, en el implícito deber del trabajador al perfeccionamiento profesional. Es una proyección del artículo 4.2.b) ET, que consagra el derecho a la promoción profesional, así como del artículo 5.e) ET, que impone al trabajador el deber básico de «contribuir a la mejora de la productividad». Este conflicto de intereses se resuelve satisfactoriamente en el artículo 52.b) ET"*[47].

---

[43] BASTERRA HERNÁNDEZ, Miguel, "La falta de adaptación a las modificaciones operadas en el puesto de trabajo como causa del despido objetivo", en RAMÍREZ MARTÍNEZ, Juan Manuel, ROMEO, Carmelo y VIQUEIRA PÉREZ, Carmen (directores), *La extinción del contrato de trabajo: Perspectiva comparada de las regulaciones italiana y española,* Valencia, Tirant lo Blanch, 2016, p. 190.

[44] VILLALBA SÁNCHEZ, Alicia, *El derecho a recibir formación de la empresa para una transición digital justa*, Cizur Menor (Navarra), Aranzadi, 2024, p. 86.

[45] *Ibidem*, p. 84.

[46] BLASCO PELLICER, Ángel, *La extinción del contrato de trabajo en la reforma laboral de 2012*, Valencia, Tirant lo Blanch, 2013, p. 117.

[4747] ALZAGA RUIZ, Icíar, "El despido del trabajador por falta de adaptación a las modificaciones técnicas en su puesto de trabajo", *Revista de derecho social,* n.º 55, 2011, p. 109. En el mismo sentido, véase GUINDO MORALES, Sara, *Caracterización jurídica y causas del despido objetivo en la normativa, doctrina y jurisprudencia tras las recientes reformas laborales,* Albolote (Granada), Comares, 2020, p. 121. También MUROS POLO, Alejandro, "Digitalización de la economía y despido tecnológico: riesgos y propuestas", en PÉREZ CALLE, Ricardo, *Empresa, economía y derecho. Oportunidades ante un entorno global y disruptivo*, Madrid, Dykinson, 2022, p. 924-925*: "El despido objetivo por inadaptación a las modificaciones técnicas resulta así de un equilibrio entre el progreso técnico empresarial, el derecho a la estabilidad en el empleo*

Como asimismo ambos, derecho y obligación, son consecuentes con los términos del artículo 23.1.d), que con relación a la promoción y formación profesional en el trabajo consagra el derecho de los trabajadores a *"la formación necesaria para su adaptación a las modificaciones operadas en el puesto de trabajo",* formación *"que correrá a cargo de la empresa"*.[48]

En este contexto, y pensando precisamente en la ciberseguridad, cabe plantearse el alcance de la expresión *"modificaciones técnicas operadas en el puesto de trabajo"*. Si se entiende de modo amplio, es de presumir que esas modificaciones no atañen en exclusiva a las introducidas de forma voluntaria por la empresa para mejorar sus procesos productivos, sino que implican igualmente las derivadas de la evolución de la tecnología que aquel haya implantado, aunque esta evolución no sea directamente atribuible a la compañía sino al devenir del progreso tecnológico. Y si las modificaciones técnicas introducidas en un puesto de trabajo implican por ley la obligatoriedad para la empresa y el correlativo derecho de la persona trabajadora a una capacitación adecuada para que este se adapte a los nuevos requerimientos de su puesto, del mismo modo, y ante la eventualidad de nuevos y continuos riesgos cibernéticos, no queda otro camino que propugnar la misma obligación empresarial y el indisociable derecho de la persona empleada a la formación y actualización permanente, habida cuenta de las graves consecuencias ya nombradas.

A tal consideración apuntan las previsiones de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)[49], que a la fecha aún está pendiente de transposición al ordenamiento español. En su artículo 7, dedicado a la *"Estrategia nacional de ciberseguridad"*, esta Directiva establece que los Estados deben adoptar políticas de *"promoción y desarrollo de la educación y la formación en materia de ciberseguridad, capacidades de ciberseguridad, sensibilización e iniciativas de investigación y desarrollo, así como orientaciones sobre buenas prácticas y controles en materia de ciberhigiene, destinadas a los ciudadanos, las partes interesadas y las entidades"*.

y el derecho a la formación profesional del trabajador, instaurando al despido objetivo por dicha causa como el último recurso utilizado".

[48] GUINDO MORALES, Sara, *ob. cit.*, p. 130: *"La realización del curso de reconversión o perfeccionamiento profesional se encuentra directamente relacionada con el artículo 23.1.d) [ET] que regula la «promoción y formación en el trabajo»"*

[49] Directiva NIS 2 por sus siglas en inglés.

No obstante, pese a que la Directiva SRI 2 incide en la trascendencia de la formación como medida esencial en la gestión de los riesgos de ciberseguridad, sus prevenciones continúan siendo insuficientes por cuanto el elenco de *"Medidas para la gestión de riesgos de ciberseguridad"* que dispone su capítulo IV se limita, en términos de obligatoriedad, a las entidades esenciales e importantes[50]. Solo para estas determina la Directiva que los Estados miembros garantizarán que sus órganos de dirección deban *"asistir a formaciones"*, optando para el resto de su fuerza laboral por una mera recomendación de que se aliente a las compañías esenciales e importantes a ofrecer *"formaciones similares a sus empleados periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad"*. Ninguna alusión, por supuesto, a entidades de menor tamaño o criticidad, aunque estén igualmente expuestas a los peligros del ciberespacio.

A su semejanza, el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad[51] que se encuentra en trámite para la transposición de la Directiva SRI 2, limita la obligatoriedad de la formación en su artículo 14.2 a la plantilla (miembros de los órganos de dirección y resto del equipo de trabajo) de las entidades esenciales e importantes. Bien es cierto que, aunque la norma se circunscribe al personal de estas compañías, sí incorpora dos condiciones que se muestran relevantes a los fines que aquí se argumentan: establece la formación en ciberseguridad como preceptiva (los miembros de los órganos de dirección *"deberán recibir"* la formación y *"deberán organizar"* formaciones similares para sus empleados) y le atribuye la cualidad de formación profesional continua y permanente, al disponer que, en todo caso y para todo el personal, debe tener carácter periódico.

En el plano nacional, la Ley 3/2023, de 28 de febrero, de Empleo, formula en su artículo 33 los fines del sistema de formación en el trabajo, entre los que, a los efectos que aquí se tratan, destacan los de mejorar las competencias digitales de las personas trabajadoras (apartado 2.c), acompañar los procesos de transformación digital (apartado 2.i) e impulsar la formación programada por las empresas para responder a las necesidades específicas de formación más inmediatas y cercanas a empresas y personas trabajadoras (apartado

[50] Definidas en el artículo 3 de la propia Directiva SIR 2. Tal y como expresa el Considerando 56 de la norma, se trata de dos categorías que clasificarán a las empresas *"en función del grado de criticidad de sus sectores o del tipo de servicio que prestan, así como de su tamaño"*.

[51] Disponible en: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf; consulta: 21.01.25. Referencia del Consejo de Ministros de 14.01.2025, disponible en: https://www.lamoncloa.gob.es/consejodeministros/referencias/paginas/2025/20250114-referencia-rueda-de-prensa-ministros.aspx; consulta: 21.01.2025.

2.j). Ahora bien, ello no deja de ser más que una plausible aspiración si no se traslada al ámbito de lo práctico.

Algo más concluyente en este aspecto resulta ser el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que en su disposición adicional primera se refiere expresamente a la formación, estableciendo la obligatoriedad para el CCN[52] y el Instituto Nacional de Administración Pública de desarrollar programas de sensibilización, concienciación y formación para *"asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad"*, si bien, teniendo en cuenta el ámbito de aplicación de esta norma, los programas estarán dirigidos únicamente al *"personal de las entidades del sector público"*.

La insuficiencia de previsión normativa en lo tocante a los riesgos cibernéticos introduce, asimismo, otra cuestión debatida por la doctrina científica sobre el alcance del derecho a la formación en la empresa, y su consideración o no como parte indisoluble del derecho fundamental a la educación consagrado en el artículo 27 de la Constitución Española. Sobre el particular, la doctrina defiende que *"la formación profesional es «una manifestación del derecho a la educación», como cualquier otro tipo de enseñanza"* [53], y que *"la inclusión del derecho a recibir formación profesional de la empresa en el derecho fundamental a la educación constituye un presupuesto ineludible para evitar la pérdida del empleo"*[54].

Uno de los puntos críticos de este debate se centra en concluir si es únicamente función de los poderes públicos acometer la labor de garantizar la formación profesional y técnica de las personas trabajadoras, o si también ha de considerarse un auténtico derecho de estas en su relación laboral, y con qué alcance, con la correlativa obligación de la empresa de suministrarla. Y en cuanto a la dimensión práctica, otro aspecto esencial de la controversia estriba precisamente en el ya planteado aquí sobre el derecho de la persona trabajadora a recibir formación de la empresa para evitar la pérdida de su empleo[55], especialmente en materia de alto riesgo como es la ciberseguridad. Ello sin perder la perspectiva sobre las muy diferentes consecuencias que una conclusión o la contraria tiene para la persona empleada[56].

---

[52] Centro Criptológico Nacional.

[53] ROMERO RÓDENAS, María José, "Dos derechos necesariamente hermanados: El derecho al trabajo y el derecho a la educación", *Revista Galega de Dereito Social,* n.º 15, 2022, p. 54 (disponible en: http://revistagalegadedereitosocial.gal/index.php/RGDS/article/view/147; consulta: 28-10-2024).

[54] VILLALBA SÁNCHEZ, Alicia, *ob. cit.*, p. 184.

[55] *Ibidem.*

[56] Diferente es, obviamente, la consecuencia de un despido improcedente que el de otro nulo, puesto que solo el segundo asegura la conservación del empleo. VILLALBA SÁNCHEZ, Alicia, *ob. cit.*, p. 184-185.

El derecho a recibir formación de la empresa tiene una dimensión mucho más amplia que la estrictamente referida a la seguridad informática y excede del objeto de este trabajo alcanzar una conclusión sobre el particular. Pero lo cierto es que la práctica empresarial, cada vez más inmersa en una profunda digitalización y con una intensa dependencia tecnológica, obliga a abordarlo como una necesidad perentoria para la empresa y su plantilla. No cabe albergar duda de que las continuas transformaciones que sufre el contexto digital en el que se desenvuelven las compañías privadas y las instituciones públicas[57] convierten en profundamente inexcusable la implantación en todas ellas de un catálogo de acciones formativas permanentes dirigidas a adiestrar a las personas trabajadoras para defenderse y defender a toda la organización de ataques informáticos. Se trata de una urgente necesidad para la empresa y asimismo para sus equipos de trabajo, porque no hay mayor peligro en materia de ciberseguridad que el desconocimiento y la ignorancia.

Con todo, la legislación positiva y la doctrina judicial, aplicadas a las actuales circunstancias de acelerado desarrollo tecnológico, ofrecen fundamentos más que sólidos para colegir que el derecho a la formación continua en materia de ciberseguridad trasciende a la consideración de necesidad o recomendación, para adquirir la cualidad de auténtico derecho de las personas trabajadoras en la relación laboral, espejo de una obligación legal de la empresa.

Como ya se ha expuesto, el argumento más firme que sustenta esta hipótesis es el escenario contemplado en el artículo 52.b ET, que contiene una doble obligación legal en la relación laboral. Incorpora, por un lado, la de la empresa de ofrecer a su personal una actividad formativa que le permita adaptarse a las modificaciones técnicas[58] que aquél haya decidido introducir en el puesto de trabajo para mejorar la productividad y competitividad de la empresa. Y a su vez, esta previsión genera la obligación legal de la persona trabajadora de cursar la formación con aprovechamiento[59] para evitar la extinción de su contrato[60], y su paralelo derecho a recibir el curso formativo que le proporcione la cualificación necesaria, en coherencia con las previsiones de los artículos 4.2.b) y 23.1.d) ET.

En este contexto, el punto de partida no es otro que la decisión empresarial, adoptada en ejercicio del poder de dirección, de poner a disposición de su personal los medios técnicos

[57] Sea cual sea su tamaño, sector o área de actividad.

[58] Sin olvidar que han de revestir la condición de razonables.

[59] Salvo que la persona empleada se adapte por sus propios medios a las modificaciones técnicas. Véase VILLALBA SÁNCHEZ, Alicia, *ob. cit.*, p. 97

[60] Posibilidad que se habilitaría para la empresa en caso de inadaptación de la persona trabajadora a las modificaciones.

necesarios para realizar su labor, lo que sitúa a este en un entorno de permanente transformación y rápida evolución tecnológica al que debe adaptarse de forma constante, pues el escenario de riesgos cibernéticos que conlleva la ejecución de tareas en el plano digital es continuamente cambiante. Cabe concluir, en consecuencia, que el derecho a la formación profesional periódica y permanente en materia de ciberseguridad es parte indisociable del derecho de la persona trabajadora a la formación para adaptarse a las modificaciones técnicas introducidas por voluntad de la empresa, y responde a la misma finalidad defensiva de evitar la pérdida del empleo por indebida utilización de los medios tecnológicos de aquella. No puede ser de otra forma, pues si se considera exigible a la persona trabajadora la obligación de conocer la tecnología para poder desarrollar su labor en un entorno de competitividad empresarial, igualmente razonable resulta entender que tenga el correlativo derecho de ser adiestrado para conocer sus peligros, efectos y consecuencias, con objeto de prevenir y mitigar sus riesgos.

A tal consideración apunta del mismo modo la jurisprudencia cuando penaliza a la empresa que no ha adoptado las oportunas medidas para evitar o, al menos, minimizar los riesgos de la tecnología puesta en manos de sus equipos de trabajo, que no pueden decidir otra cosa que utilizarla, a riesgo de ser sancionados, incluso, con el despido. La posibilidad de declaración de improcedencia o nulidad de las medidas disciplinarias impuestas en un contexto de falta de capacitación previa sustenta la hipótesis de que la responsabilidad empresarial va más allá de un deber moral, constituyendo una auténtica obligación legal de proporcionar la formación en ciberseguridad.

En definitiva, si de forma general la participación en acciones formativas por parte de la persona trabajadora es un derecho que le concierne en la relación de trabajo con vías a favorecer su mayor empleabilidad (ex artículo 4.2.b) ET), el derecho a la formación en ciberseguridad se inserta en un estadio superior y cualificado, debiendo ser calificado necesariamente de derecho exigible y de paralela obligación legal, por cuanto resulta decisivo en las actuales circunstancias para la conservación del empleo de la persona empleada y para la protección de la empresa en su conjunto[61], dados los intereses en juego.

Desde esta perspectiva, pese a todo, ha de puntualizarse que el hecho de que la formación en ciberseguridad deba ser periódica y alcanzar a todos los integrantes de la fuerza laboral de la empresa no obsta para considerar que la estructura de la formación no tiene por qué ser única y universal. Las diferentes funciones y el distinto nivel de exposición a los riesgos cibernéticos de los diversos puestos de trabajo justifican que la formación haya de ser adaptada a cada una de esas situaciones, por lo que tanto el derecho de la persona

[61] Empresa, plantilla, clientes y usuarios. Y, dependiendo del nivel de criticidad de la compañía, pueden estar en riesgo, además, la seguridad nacional y otros intereses generales de gran peso.

trabajadora como la correlativa obligación legal de la empresa deben ser proporcionales y acompasados al grado de exposición de cada puesto a las amenazas cibernéticas. No debe desdeñarse el hecho de que, aun siendo muy pocas, todavía existen ocupaciones que no precisan de la tecnología para su desempeño.

Y, en coherencia con lo anterior, viene al caso mencionar que la impartición obligatoria de la formación, y su recíproco seguimiento obligado por cada integrante de la plantilla en atención a las exigencias de su propio puesto de trabajo, deben conjugarse con el derecho a la no discriminación por motivo de género, edad, sexo, discapacidad o cualquier otra circunstancia prohibida por el ordenamiento[62]. A la hora de poner a disposición del equipo de trabajo los oportunos planes formativos en materia de ciberseguridad, solo cuestiones como el nivel de exposición al riesgo o las diferentes funciones de cada puesto pueden ser determinantes del derecho de cada profesional a participar en aquellos, sin que otros sesgos puedan excluir a personas individuales o a determinados colectivos por causas ajenas al uso y manejo de la tecnología, o por motivos que no se deriven objetivamente de tal utilización[63].

A mayor abundamiento, no conviene pasar por alto la dimensión que la ciberseguridad puede alcanzar en términos de prevención de riesgos laborales. La circunstancia de que el V AENC inserte en el ámbito de la seguridad y salud en el trabajo la recomendación de incluir programas formativos sobre los riesgos de uso de las nuevas tecnologías en la relación laboral -en los términos ya expuestos en el anterior epígrafe-, entronca con la formación obligatoria que el artículo 19 ET establece a cargo de la empresa cuando sus profesionales han de afrontar las transformaciones tecnológicas que se introducen en el proceso productivo. Obligación que se reitera en el artículo 19.1 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, cuyo segundo párrafo incide en la pertinencia de que la formación sea constante y continua, exigiendo no solo que esté *"centrada específicamente en el puesto de trabajo o función de cada trabajador"*, sino que además deba adaptarse *"a la evolución de los riesgos y a la aparición de otros nuevos y repetirse periódicamente, si fuera necesario"*. Sin duda es un argumento más que

[62] Enumeradas en el artículo 2 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación. En el artículo 3 de la misma ley se menciona expresamente la promoción y formación profesional en el ámbito del empleo público y privado, por cuenta propia o ajena.

[63] A lo que se debe añadir la necesaria evitación de discriminación por causa de la metodología de la actividad formativa, o por el lugar y tiempo de su impartición, situaciones que pueden penalizar o excluir a personas con mayores barreras tecnológicas. Es el caso de grupos que por razón de edad tengan competencias digitales limitadas, o de colectivos con menor disponibilidad de tiempo por necesidades de conciliación, o con menores recursos económicos que les impidan el seguimiento de planes formativos en remoto por carecer de dispositivos digitales propios. Sobre este particular, véase VILLALBA SÁNCHEZ, Alicia, *ob. cit.*, p. 187-188.

refuerza el derecho de la persona trabajadora a obtener y actualizar su formación en materia de seguridad informática.

4. Conclusiones

I. La regulación del uso de las tecnologías de la información y de la comunicación en el ámbito laboral es una necesidad derivada del marco de seguridad jurídica en el que precisan desenvolverse las empresas y su personal, certidumbre que no está plenamente garantizada sin una sólida política de ciberseguridad. Aunque no conviene prescindir de la implantación de tecnologías avanzadas y de personal especializado en ciberseguridad como primera barrera de autoprotección frente a ataques informáticos, lo cierto es que ni siquiera las herramientas más punteras resultarán suficientes si la fuerza laboral de una empresa no está entrenada para reconocerlos y repelerlos.

Por ello, la formación profesional en materia de ciberseguridad se debe erigir en puntal esencial de la estrategia de autoprotección de las empresas, seguido a muy corta distancia por la sensibilización de sus equipos de trabajo. Tan importante es la impartición de adiestramiento específico sobre los riesgos cibernéticos como la concienciación de las personas empleadas acerca de las políticas de seguridad de las compañías, para que entiendan las instrucciones y sus motivos y las asuman como propias. Se trata de crear una cultura de ciberseguridad firme y consolidada, ya que conocer las amenazas y sus consecuencias es esencial para afrontar ataques informáticos y evitar colaboraciones con los ciberdelincuentes, sean intencionadas o involuntarias.

La respuesta a las amenazas cibernéticas no será suficiente si se centra solo en sancionar conductas negligentes o dolosas de las personas empleadas que no cumplan la política de ciberseguridad de la empresa. Más importante que la actitud reactiva ante las amenazas del ciberespacio es la actitud proactiva centrada en la prevención, pues el mejor escenario es que el ataque no prospere. Al tiempo, si la vertiginosa evolución de la tecnología ocasiona una rápida obsolescencia de los conocimientos sobre seguridad informática, la formación de los usuarios de las nuevas tecnologías ha de ser permanente para que puedan adaptarse a la sofisticación de los ataques.

II. El suministro de formación permanente a la plantilla en cuestiones de seguridad informática ha de configurarse como una obligación legal para la empresa, puesto que no es factible exigir a los equipos de trabajo una conducta responsable sin una previa preparación sobre los riesgos de la tecnología y las técnicas para evitarlos y repelerlos. Mayor responsabilidad tendrá la empresa que no adopte las medidas preventivas necesarias para evitar riesgos cibernéticos previsibles, con el consiguiente resultado de improcedencia o nulidad de las eventuales sanciones disciplinarias impuestas en este

contexto. De ello dan muestra las resoluciones judiciales dictadas en supuestos de incidentes informáticos sucedidos por mal uso de la tecnología, en los que no se contaba con una previa capacitación para afrontar potenciales ataques informáticos.

Correlativamente, la obligación de proporcionar formación permanente en el área de la seguridad informática sustenta el derecho de la persona trabajadora a recibirla. Si el artículo 52 b) ET consagra el derecho de esta a obtener a cargo de la empresa la formación que le capacite para adaptarse a las modificaciones técnicas operadas en su puesto de trabajo, es de entender que en estos cambios tecnológicos han de considerarse comprendidos tanto los introducidos voluntariamente por la empresa en aras de su desarrollo y progreso como los derivados de avances tecnológicos o de las necesidades de seguridad informática.

El peligro de incurrir en conductas que puedan ocasionar daño a la empresa o a terceros sitúa a las personas trabajadoras en un contexto de riesgo propio, ante la contingencia de ser sancionadas por ello, incluso con la pérdida de su puesto de trabajo, lo que refuerza la necesidad de reivindicar su derecho a estar permanentemente formadas e informadas en materia de seguridad informática. Desde esta perspectiva es justificado sostener que el derecho a la formación en ciberseguridad forma parte inherente del derecho de la persona trabajadora a recibir formación para adaptarse a las modificaciones técnicas introducidas por la empresa, ya que son estas las que sitúan a toda la compañía en su conjunto en un escenario de constante exposición a las amenazas cibernéticas. Entorno de riesgo que, por añadidura, no es una foto fija sino un contexto en permanente transformación, lo que requiere de un aprendizaje continuo.

La estructura de la formación debe acomodarse a las necesidades de cada puesto de trabajo, pues la exigencia de capacitación será en cada caso proporcional al nivel de exposición que experimente el profesional en virtud de las herramientas tecnológicas que deba utilizar para desarrollar su labor, y de los intereses que pueda poner en riesgo en la realización de su tarea. Esa utilización de herramientas tecnológicas y dispositivos conectados como instrumento de trabajo o como sistema de comunicación, gestión y manejo de información, ha de imperar como criterio de impartición de la formación, descartándose cualquier otro que implique discriminación o provoque la exclusión de determinados individuos o colectivos.

III. A pesar de los riesgos y de la consolidada conciencia general de la necesidad de formación permanente sobre amenazas cibernéticas, la legislación social aún no está adaptada al nuevo escenario tecnológico que afecta profundamente a las relaciones laborales. Esta anomia en materia de ciberseguridad aboca a reclamar un papel activo de la negociación colectiva en la regulación del derecho de la persona trabajadora a la

formación permanente sobre cuestiones de seguridad informática y el correlativo deber de la empresa de proporcionarla. En cualquier caso, el legislador no puede dar la espalda a una realidad que ya no tiene vuelta atrás. El proceso de digitalización en el que la sociedad se encuentra inmersa es irreversible, y de igual forma que la ley refuerza la protección del consumidor como parte más débil de la contratación mercantil, la legislación laboral ha de dar la misma contundente respuesta a las contingencias que la digitalización está introduciendo en la relación de trabajo, en la que es la persona trabajadora quien ocupa la posición más vulnerable.

5. Bibliografía

AA. VV., *Guardianes digitales para un crecimiento sostenible: Ciberseguridad y protección ciudadana en la era de la transformación digital,* VAQUERO GARCÍA, Alberto (director), Madrid, Consejo Económico y Social de España, 2024.

ÁLVAREZ CUESTA, Henar, "La ciberseguridad en la empresa: Una aproximación desde el derecho del trabajo", *Derecho de las relaciones laborales*, nº 7, 2019, p. 682-690.

ALZAGA RUIZ, Icíar, "El despido del trabajador por falta de adaptación a las modificaciones técnicas en su puesto de trabajo", *Revista de Derecho Social,* nº 55, 2011, p. 109-139.

BALLESTER CASANELLA, Blanca, "Los nuevos desafíos que plantean las nuevas tecnologías en el ámbito de la desvinculación laboral", *Revista de Derecho, Empresa y Sociedad (REDS),* nº. 22-23, 2023, p. 43-58 (disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9294271; consulta: 22.10.2024).

BASTERRA HERNÁNDEZ, Miguel, "La falta de adaptación a las modificaciones operadas en el puesto de trabajo como causa del despido objetivo", en RAMÍREZ MARTÍNEZ, Juan Manuel, ROMEO, Carmelo y VIQUEIRA PÉREZ, Carmen (directores), *La extinción del contrato de trabajo: Perspectiva comparada de las regulaciones italiana y española,* Valencia, Tirant lo Blanch, 2016, p. 181-190.

BLASCO PELLICER, Ángel. *La extinción del contrato de trabajo en la reforma laboral de 2012,* Valencia, Tirant lo Blanch, 2013.

DE CASTRO MEJUTO, Luis Fernando, "La formación profesional de los trabajadores de edad madura frente a la brecha digital", en MELLA MÉNDEZ, Lourdes (directora) y FERREIRO REGUEIRO, Consuelo (coordinadora), *La formación profesional para la*

empresa y la sociedad del siglo XXI: Puntos críticos, Cizur Menor (Navarra), Aranzadi, 2023, p. 315-348.
GUINDO MORALES, Sara, *Caracterización jurídica y causas del despido objetivo en la normativa, doctrina y jurisprudencia tras las recientes reformas laborales,* Albolote (Granada), Comares, 2020.

MUÑOZ RUIZ, Ana Belén, "Cómo afecta la ciberseguridad a los derechos laborales de las personas empleadas y sindicatos. Comentario a la Sentencia del Tribunal Supremo 1033/2020, de 25 de noviembre", *Revista de Trabajo y Seguridad Social*, nº 459, 2021, p. 207-219 (disponible en: https://revistas.cef.udima.es/index.php/rtss/article/view/2404; consulta: 21.10.2024).

MUROS POLO, Alejandro, "Digitalización de la economía y despido tecnológico: riesgos y propuestas", en PÉREZ CALLE, Ricardo, *Empresa, economía y derecho. Oportunidades ante un entorno global y disruptivo*, Madrid, Dykinson, 2022, p. 915-937.

ROMERO RÓDENAS, María José, "Dos derechos necesariamente hermanados: El derecho al trabajo y el derecho a la educación", *Revista Galega de Dereito Social,* nº 15, 2022, p. 45-64 (disponible en: http://revistagalegadedereitosocial.gal/index.php/RGDS/article/view/147; consulta: 28.10.2024).

VILLALBA SÁNCHEZ, Alicia, *El derecho a recibir formación de la empresa para una transición digital justa*, Cizur Menor (Navarra), Aranzadi, 2024.