universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2019/2020

DISPOSITIVOS MÓVILES PROPIEDAD DEL TRABAJADOR (BYOD): SU IMPACTO EN LOS DERECHOS LABORALES DIGITALES

MOBILE DEVICES OWNED BY THE WORKER (BYOD): THEIR IMPACT ON DIGITAL LABOR RIGHTS

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR/A: D. LOMBARDO ALEJANDRO ARDÓN MEJÍA

TUTOR/A: DRA. Dª. SUSANA RODRÍGUEZ ESCANCIANO

AGRADECIMIENTOS

Gracias a Dios por ayudarme a cumplir el sueño de estudiar un posgrado en España, a la Fundación Carolina y al Instituto Nacional de Ciberseguridad (INCIBE) por ayudarme a materializarlo con la beca que me han brindado, a la Universidad de León por ser mi casa de estudios durante el curso 2019/2020 y a mi tutora la Profa. Dra. Susana Rodríguez Escanciano, por su valiosa colaboración, tiempo y buena disposición en la realización de este trabajo.

DEDICATORIA

A mis padres y hermanas, por ser el motor con el cual he conducido mi camino académico y profesional todos estos años, a mis amistades, por siempre estar pendiente de mi, aunque nos encontrábamos a miles de kilómetros de distancia, y a Juli, gracias por los momentos compartidos, tu transferencia de conocimiento y tu gran apoyo.

ÍNDICE

RESUMEN

Este trabajo recoge una recopilación de situaciones excepcionales que ocurren en el ámbito laboral a raíz de los cambios tecnológicos que las empresas adoptan, y que surgen como producto de la transformación digital a la que estas se enfrentan hoy en día, centrando la atención en una de sus manifestaciones: el *Bring Your Own Device* (BYOD), que puede definirse como el uso de dispositivos móviles personales propiedad del trabajador para fines laborales. Con el análisis de esta tendencia tecnológica, se profundiza en las consecuencias de la incorporación de dichos dispositivos durante la jornada de trabajo, pues esto trae consigo una serie de riesgos jurídico-laborales y técnicos (en materia de seguridad de la información) que tanto los empleadores como los trabajadores deben de tomar en cuenta para su correcto uso e implementación.

Con este trabajo, el lector partirá de una visión general sobre las relaciones laborales en la era digital y cómo las tecnologías de la información y la comunicación juegan un papel esencial en ellas, dando paso a conocer los aspectos técnicos del BYOD, y a su vez un análisis e interpretación del mismo desde una serie de escenarios donde se acercará a diferentes preceptos normativos del ordenamiento jurídico español, denotando el impacto que esta tendencia puede generar en los derechos fundamentales y laborales digitales de los trabajadores. Todo ello sin olvidar el estudio de diferentes recomendaciones en materia técnica, como ser políticas de seguridad y configuración de herramientas tecnológicas que en su conjunto ayudan a materializar una correcta implementación del BYOD en la empresa.

ABSTRACT

This work collects a compilation of exceptional situations that occur in the workplace as a result of the technological changes that companies adopt, and that arise as a product of the digital transformation that they face today, focusing attention on one of its manifestations: Bring Your Own Device (BYOD), which can be defined as the use of personal mobile devices owned by the worker for work purposes. With the analysis of this technological trend, the consequences of the incorporation of said devices during the working day are explored, as this brings with it a series of legal-labor and technical risks (in terms of information

security) that both employers and workers must take into account for its correct use and implementation.

With this work, the reader will start from a general vision of labor relations in the digital age and how information and communication technologies (ICTs) play an essential role in them, thus giving way to know the technical aspects of the BYOD, and in turn an analysis and interpretation of it from a series of scenarios where it will approach different normative precepts of the Spanish legal system, denoting the impact that this trend can generate on the fundamental and digital labor rights of workers. All this without forgetting the study of different recommendations in technical matters, such as security policies and configuration of technological tools that together help to materialize a correct implementation of BYOD in the company.

PALABRAS CLAVE

Relaciones laborales, BYOD, dispositivos móviles personales, derechos fundamentales, derechos laborales digitales, riesgos jurídico-laborales, políticas de seguridad.

KEYWORDS

Labor relations, BYOD, personal mobile devices, fundamental rights, digital labor rights, legal and employment risks, security policies.

OBJETO DEL TRABAJO

El presente trabajo aborda las dificultades jurídico-laborales y técnicas que conlleva la adopción e implementación de la tendencia tecnológica *Bring Your Own Device* (BYOD) en las empresas, consistente en la utilización de dispositivos móviles personales propiedad del trabajador para fines laborales. Analizando así, bajo la perspectiva de lo normado en el ordenamiento jurídico español, una serie de situaciones alrededor de los derechos fundamentales y laborales digitales de los trabajadores, haciendo un notable hincapié en el impacto que esta tendencia genera en ellos.

Por lo tanto, a lo largo de las páginas de este trabajo, nos centraremos en abordar el BYOD desde diferentes aristas que nos ayudarán a conocerlo y estudiarlo desde varios preceptos normativos en materia laboral, profundizando en las lagunas jurídicas existentes alrededor de derechos fundamentales como el de la intimidad, el secreto de las comunicaciones, la propia imagen, la protección de datos, y laborales digitales como el derecho a la desconexión digital; abordándolo también alrededor de una serie de recomendaciones técnicas que en su conjunto ayudan a hacer frente a esta tendencia al momento de implementarla en la empresa.

Es así, que como objetivo general de este trabajo buscamos analizar el impacto jurídico-laboral del BYOD en los derechos fundamentales y laborales digitales de los trabajadores. A su vez, para cumplimentarlo se cuenta con una serie de objetivos específicos, que en su conjunto nos ayudarán a llegar a ese cometido. Estos son:

- Explicar los cambios sufridos por las relaciones laborales en la era digital y el despliegue tecnológico que estas acarrean.
- Definir la tendencia del BYOD, sus características, ventajas y riesgos.
- Exponer lo actualmente regulado en materia laboral con respecto al poder de control empresarial y uso de dispositivos tecnológicos en la jornada de trabajo.
- Delimitar los derechos fundamentales y laborales digitales que se pueden ver impactados por el BYOD.
- Brindar una serie de recomendaciones a nivel técnico-empresarial para una correcta implementación del BYOD.

METODOLOGÍA

De acuerdo con la lectura del tema y objetivos, esta investigación se apoyó del paradigma cualitativo, haciendo uso del enfoque metodológico lógico deductivo, combinado con una perspectiva crítica ante los diferentes escenarios propuestos a lo largo del trabajo.

En consecuencia, se siguieron tres etapas durante el desarrollo del trabajo:

1. **Fase exploratoria:** cuyo objetivo es documentar la realidad que se va a analizar y planificar el encuadre más adecuado para realizar la investigación. Se realiza a través de la revisión de toda la documentación existente y disponible sobre el tema (es decir: leyes, sentencias de tribunales, artículos doctrinales, o cualquier otra evidencia material, que permita reconstruir y contextualizar el proceso o tema de análisis, previo a la lectura crítica y reflexiones deductivas). Esta fase, permitió hacerse preguntas con base en la descripción, que se emplea en cada uno de los apartados o capítulos del trabajo.

2. **El muestreo de caso crítico:** se edifica sobre la base de elegir una situación general que permite ganar comprensión sobre una condición hipotética sometida a análisis crítico por parte del investigador, y como resultado de un juicio o descripción particular; por otro lado, permite develar aspectos completamente invisibles de los temas.

En este trabajo, este tipo de muestro fue útil, para dar respuesta a las premisas generales, y con ello, lograr plantear recomendaciones sobre el impacto y la correcta implementación del BYOD, sobre todo, desde la compresión del ordenamiento jurídico español y demás normativa de la nueva era tecnológica digital.

3. **Plan de análisis:** se hizo uso del análisis de contenido, es decir, lograr abstraer los elementos o ideas claves de cada documentación revisada, para establecer el análisis y lectura deductiva que permitió explicar cada uno de los capítulos. Por otro lado, también permitió, construir representaciones o soluciones jurídicas importantes, para que futuros lectores de este trabajo, puedan comprender el impacto del BYOD en los derechos laborales digitales de los trabajadores.

I. RELACIONES LABORALES EN LA ERA DIGITAL

Transcurridas las dos primeras décadas del siglo XXI, sin duda alguna estamos viviendo inmersos en una sociedad altamente hiperconectada e hipercomunicada de ámbito globalizado[1].

En palabras de Juana Mª Serrano García, la transformación digital[2] (también denominada cuarta revolución industrial) "es ya una realidad que afecta a todos los planos de la vida de las personas, con repercusiones tanto a nivel social como económico"[3].

Asimismo, el apartado IV del Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos Digitales (en adelante, LOPDyGDD)[4], admite que internet "se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva", y que "una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad".

Por consiguiente, y debido a esta transformación digital que se ha desplegado a lo largo de los últimos años, surge una disrupción tecnológica que ha llegado a cambiar la forma cotidiana de hacer y ver las cosas, encontrando como pilar y exponente fundamental los centros de trabajo, y alterando desde la realización de métodos y procesos a nivel de negocio, las formas de trabajar y de organizar la actividad, hasta la propia naturaleza jurídica de las relaciones laborales y las condiciones en que estas se desempeñan[5].

---

[1] BAZ RODRIGUEZ, Jesús. *Privacidad y protección de datos de los trabajadores en el entorno digital.* Madrid: Wolters Kluwer, 2019, pág. 15.

[2] La transformación digital es lo que sucede cuando las empresas adoptan nuevas e innovadoras formas de hacer negocios con base en los avances tecnológicos. RED HAT. *¿Qué es la transformación digital?* [en línea]. Disponible en: https://www.redhat.com/es/topics/digital-transformation/what-is-digital-transformation

[3] SERRANO GARCÍA, Juana Mª. *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia.* Albacete: Bormazo, 2019, pág. 9.

[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

[5] PÉREZ DE LOS COBOS ORIHUEL, Francisco. *Nuevas tecnologías y relación de trabajo*. Valencia: Tirant lo Blanch, 1990, págs. 19 y ss.

Esto último es posible dado a la extensa propagación del uso de las tecnologías de la información y la comunicación (en adelante, TICs) en el ámbito empresarial, las cuáles, juegan un papel de cambio sumamente notorio e importante para asimilar que todo lo que hemos logrado conocer y entender con anterioridad, hoy en día no es ni un poco a lo que nos enfrentamos (y llegaremos a enfrentar) con la incursión de las nuevas tecnologías.

En este sentido y a efecto de modelar un concepto que nos ayude a abordar la temática de este apartado, entenderemos por la existencia de una relación laboral (o también relación de trabajo), lo expresado por la Organización Internacional del Trabajo (en adelante, OIT): "la relación de trabajo es una noción jurídica de uso universal con la que se hace referencia a la relación que existe entre una persona, denominada «el empleado» o «el asalariado» (o, a menudo, «el trabajador»), y otra persona, denominada el «empleador», a quien aquélla proporciona su trabajo bajo ciertas condiciones, a cambio de una remuneración"[6].

De igual manera, y con el objetivo de contar con otra referencia, destacamos en palabras de Julio Grisolia, reconocido laboralista argentino, que una relación de trabajo "es una situación de hecho que manifiesta una relación de dependencia […] que, sin perjuicio del contrato de trabajo […], la relación de trabajo es la prestación efectiva de las tareas, las que pueden consistir en la ejecución de obras, actos o servicios" [7].

Con referencia al ordenamiento jurídico español, si nos remitimos al 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 adelante, ET)[8], no encontraremos una definición jurídica exacta de lo que es una relación laboral. Sin embargo, los apartados 1 y 2 del art. 1 de dicha ley española nos hace alusión a que "esta ley será de aplicación a los trabajadores que voluntariamente presten sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o

[6] ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *La Relación de Trabajo* [en línea]. 2006, pág. 3. Disponible en: http://www.ilo.org/public/spanish/standards/relm/ilc/ilc95/pdf/rep-v-1.pdf

[7] GRISOLIA, Julio Armando. *Manual de Derecho Laboral* [en línea]. Ciudad Autónoma de Buenos Aires: Abeledo Perrot, 2019, pág. 46. Disponible en: https://proview-thomsonreuters-com.digitalbd.uade.edu.ar/

[8] 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. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

empresario", delimitando de igual manera que, un empleador o empresario serán "todas las personas, físicas o jurídicas […] que reciban la prestación de servicios de las personas referidas en el apartado anterior", de esta manera, aunque lo expuesto no sea un concepto explícito, la correlación de ambos preceptos serán fundamentales para construir bajo las características que mencionan, una relación de trabajo.

Con lo antes mencionado y retomando la finalidad de este apartado con respecto al impacto que las TICs generan en el ámbito laboral, cabe destacar que la ya mencionada disrupción tecnológica puede penetrar sobre todos los trabajos, sean más o menos cualificados, bajo cualquier régimen jurídico, subordinados o autónomos, privados o públicos, ejecutados en el seno de uno u otro tipo de empresas, desde las grandes corporaciones transnacionales a las micro-estructuras; en fin afecta a todo tipo de relación laboral[9], esto debido a que el ámbito de aplicación de las TICs es cada vez más extenso y por consecuencia menos propenso a ser omitido por las empresas.

Es así que destacamos como hecho, que las relaciones laborales en la era digital han cambiado mucho por la influencia desvirtuadora de las TICs, por una parte, principalmente por afectar a un número considerable de condiciones laborales básicas, como ser el tiempo de trabajo, facultades organizativas y de control empresarial, prevención de riesgos laborales, entre otras[10], y por otra, ya que por ejemplo, aunque nos hemos enfrentado a muchos casos en los que la fuerza de trabajo humana se ha visto reemplazada por innovaciones tecnológicas (como la robótica, inteligencia artificial, algoritmos, etc.), generando así menos puestos de trabajos físicos, de igual manera, el auge de nuevas tecnologías ponen entre dicho que se necesita de una intervención humana capacitada para poder interactuar con ellas, haciendo

[9] CRUZ VILLALÓN, Jesús. "Las transformaciones de las relaciones laborales ante la digitalización de la economía". *Temas Laborales: Revista andaluza de trabajo y bienestar social* [en línea]. 2017, núm. 138, pág. 16. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6552388

[10] DEL REY GUANTER, Salvador. "Relaciones laborales y nuevas tecnologías: reflexiones introductorias", en AA.VV. (DEL REY GUANTER, Salvador, Dir. y LUQUE PARRA, Manuel, Coord.): *Relaciones Laborales y Nuevas Tecnologías* [en línea]. Madrid: La Ley, 2005, pág. 3. Disponible en: https://books.google.es/books/about/Relaciones_laborales_y_nuevas_tecnolog%C3%AD.html?id=osR5WCpKxX8C&redir_esc=y

así que se generen puestos de trabajo con altas expectativas de crecimiento y capacitación continua.

Por cuanto a toda esta manifestación de transformación a las relaciones laborales tradicionales, es evidente suponer también la existencia de pérdida del concepto de trabajo tradicional con presencia física del trabajador, hacía nuevas figuras "virtuales o digitales" caracterizadas por la ausencia del mismo en las dependencias empresariales y creando a su vez la denominada "dependencia tecnológica"[11], que aunque puede facilitar y flexibilizar la modernización de la organización del trabajo para las empresas y organizaciones, dándoles así a sus trabajadores una mayor autonomía en la realización de sus tareas, supone también para los mismos, el conflicto de tratar de conciliar una vía de doble dirección entre la vida profesional y la vida social o personal[12].

Lo anterior no podría ser de otra forma, si aceptamos que con la transformación digital (que no ha hecho nada más que comenzar), estamos ante uno de los cambios más profundos de la organización del trabajo en la empresa y, con ello, de las relaciones laborales, impactando directamente en la ordenación jurídica de estas[13].

Por esta razón, este cambio del que estamos hablando nos conduce a pensar en ¿cómo seguirá siendo el trabajo del futuro?, ¿de qué manera se podrá regular o seguir regulando el uso de las TICs en el trabajo?, ¿el empleador está preparado para afrontar y abordar todos estos cambios?, ¿la legislación en materia será lo suficientemente capaz de evolucionar y regular todo esto a tiempo?

En respuesta a estas incógnitas, por parte del empleador será necesario no solo adoptar nuevas estrategias de negocio que impulsen y controlen el uso de las TICs en pro de seguir el camino

---

[11] ORDOÑEZ PASCUA, Natalia. "Relaciones de trabajo y ciberseguridad: nuevos retos en un futuro tecnológico incierto". *Revista General de Derecho del Trabajo y de la Seguridad Social* [en línea]. 2019, núm. 53, pág. 248. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7013608

[12] GORDO GONZÁLEZ, Luis. "El Derecho del Trabajo 2.0: la necesidad de actualizar el marco de las relaciones laborales a las nuevas tecnologías". *Revista de Información laboral* [en línea]. 2017, núm. 12, pág. 178. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6283319

[13] DEL REY GUANTER, Salvador. Relaciones laborales y nuevas tecnologías: reflexiones introductorias. cit. p. 3.

de la era digital, sino que también conocer los beneficios, el impacto y los riesgos que esto conlleva al trabajador, es decir, esta dependencia tecnológica de la que hemos hecho alusión, que tanto influirá en su quehacer institucional, y más allá de eso, que tanto se verán expuestos y/o vulnerados algunos derechos fundamentales y laborales digitales del mismo cuando estas tecnologías se vuelquen contra ellos, permitiendo así que esto sea uno de los principales retos que el derecho del trabajo y la gestión empresarial deberán afrontar en los próximos años.

A este punto resulta inevitable no estar involucrados ante la situación de conformación del protagonismo de las distintas fuentes técnicas y jurídicas que han de regular las materias resultantes de la creciente e incierta relación entre nuevas tecnologías y relaciones laborales; es por eso, que respecto al uso de las TICs en la empresa por parte de los trabajadores, y mientras que la normativa estatal y los convenios colectivos se mantienen en una posición de espera, es a nivel de empresa, mediante acuerdos e instrucciones del empleador reflejados en códigos de conductas, guías de buenas prácticas, entre otras, donde encontramos las regulaciones más precisas al respecto[14].

Mientras tanto, y en adición a lo anterior, "son las decisiones de los jueces, en la mayor parte basadas directamente en los preceptos constitucionales dedicados a los derechos fundamentales, las que están estableciendo las pautas ordenadoras en un ámbito como el de las nuevas tecnologías que está llamado a alterar sustancialmente aspectos esenciales de las relaciones laborales"[15].

[14] DEL REY GUANTER, Salvador. Op. cit. p. 8.

[15] DEL REY GUANTER, Salvador. Op. cit. p. 8.

II. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN EN EL ÁMBITO LABORAL, ¿ALIADAS O ENEMIGAS?

Cada vez, en mayor medida, el uso de las TICs proporciona una ventaja competitiva a las organizaciones, sobre todo en aquellas en las que estas se integran en la estrategia general de la propia organización[16].

Como consecuencia directa de ello, en el ambiente empresarial, la gestión tecnológica se manifiesta de una manera especialmente singular en los planes, las estrategias y las políticas de carácter estructural y tecnológico para la adquisición, uso y creación de tecnología, así como cuando se asume la innovación como eje fundamental de las estrategias de mejora y desarrollo de los negocios[17].

En este sentido, cabe indicar, que la gestión de la tecnología se ha convertido en una poderosa herramienta que se debe enmarcar dentro de los procesos generales de innovación al que están sometidas todas las empresas, gestando así, una acertada transformación digital.

Asimismo, lo anterior no desacredita que la incorporación de las TICs en el ámbito laboral tiene muchas aristas imbricadas, desde beneficios tangibles e intangibles por su correcto uso y explotación en pro de mejorar la productividad laboral por parte del trabajador (que por consiguiente impacte en beneficios propios para la empresa), hasta una serie de riesgos por un indebido control e incorporación de las mismas, que puedan llegar a afectar desde procesos de negocio, quehacer institucional de la empresa, hasta el desenvolvimiento laboral del trabajador. Esto último, en consonancia con la posible afectación de derechos fundamentales y laborales digitales que les sean concernientes a los mismos.

Bajo este escenario, y como consecuencia del mismo, se puede afirmar que las TICs, en su constante evolución, han permitido que se desarrollen nuevas herramientas para desempeñar

[16] PUYOL, Javier. *Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa* [en línea]. Valencia: Tirant lo Blanch, 2015, pág. 10. Disponible en: https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490860434

[17] PUYOL, Javier. Op. cit. p. 10.

labores profesionales de forma más eficaz y eficiente[18]; sin embargo, tal y como veremos más adelante en este trabajo, también conllevan como efecto más destacado, un auténtico "control capilar" de los trabajadores en el puesto de trabajo e incluso fuera del mismo[19]. Todo esto, debido a la alta movilidad que las TICs brindan al trabajador, donde en el entorno de trabajo se ha pasado de usar el ordenador de escritorio como principal herramienta, a utilizar dispositivos móviles como smartphones, tablets u ordenadores portátiles[20].

Sabemos que el activo más importante de una empresa es la información. Esta movilidad a la que hacemos alusión, por el constante y desbordado uso de dispositivos móviles conlleva entre otros riesgos a la posibilidad de pérdida o robo del dispositivo, y otro tipo de eventos, como la pérdida de confidencialidad de la información contenido en el mismo[21]. ¿Y que pasaría si ese dispositivo es propiedad del trabajador? Además de generarse una pérdida material, ¿el dispositivo habrá contado con todas las medidas de seguridad necesarias para resguardar la información en caso de un siniestro de este tipo?

Con todo lo anterior, no buscamos implantar una idea de que las TICs son más un error que un acierto para la gestión empresarial, pero es evidente que, hasta la fecha, tal como apunta Vicente Calle, "las empresas se esforzaban en crear entornos cerrados que garantizaran el control de su información y que les permitieran ejercitar su facultad de dirección y organización del trabajo"[22].

Ahora, ese entorno protegido y conocido se agrieta de manera natural e inevitable, y esto plantea muchos desafíos, por ejemplo, algunas cuestiones relativas a la seguridad, tales como el archivo de información fuera del entorno de la empresa (en los dispositivos y en la nube),

[18] PUYOL, Javier. Op. cit. p. 10.

[19] RODRÍGUEZ ESCANCIANO, Susana. *Derechos laborales digitales: garantías e interrogantes*. Pamplona: Aranzadi, 2019, pág. 19.

[20] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 13.

[21] PUYOL, Javier. Op. cit. p. 14.

[22] CALLE, Vicente. *BYOD, "utiliza tu dispositivo personal para trabajar", la nueva revolución* [en línea]. Disponible en: https://www.garrigues.com/es_ES/noticia/byod-utiliza-tu-dispositivo-personal-para-trabajar-la-nueva-revolucion

el uso de software no autorizado (Apps de todo tipo, no sólo profesionales, sino también personales), entre otras circunstancias concurrentes[23].

De igual manera, se han venido planteando cuestiones legales muy relevantes, ya que uno de los principios básicos fundados por la doctrina de los tribunales europeos y españoles, es que el empleador tiene legítimo derecho de control sobre esos dispositivos debido a que los mismos son propiedad de la empresa[24].

Así hace referencia la Sentencia del Tribunal Constitucional de 17 de diciembre de 2012[25], señalando que "en el marco de dichas facultades de dirección y control empresariales no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligación relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales".

Si prestamos suma atención a lo anterior, podremos distinguir claramente, que este control del empleador va más allá del "poder imperativo" que posee el mismo como figura dominante en la estructura organizacional de la empresa. También es importante subrayar que este debe tener cuidado con la vulneración de derechos fundamentales y laborales digitales, además de eso, ¿qué pasaría si ese dispositivo es propiedad del trabajador?

En respuesta a la última incógnita, estaríamos frente a lo que se conoce como *Bring Your Own Device* (en adelante, BYOD), una tendencia que será descrita y analizada desde diferentes escenarios a lo largo de este trabajo, y respecto de la cual de manera preliminar, destacamos que hace alusión a que los medios utilizados por los trabajadores ya no serán utilidad de la empresa, por lo que será necesario que estas mismas revisen contratos, procesos y políticas para ejercer correctamente ese control e incluso poder exigirlo judicialmente si

[23] CALLE, Vicente. Op. cit.

[24] CALLE, Vicente. Op. cit.

[25] STCo 241/2012, de 17 de diciembre.

fuera necesario[26], siempre y cuando no se vulneren las garantías de ciertos derechos fundamentales y laborales digitales de los trabajadores.

Por lo tanto, definir a las TICs como aliados o enemigos será totalmente proporcional al equilibrio definitivo entre beneficios y contraindicaciones que estas brindan y que deberán ser gestionados tanto por los empleadores como por los trabajadores, con políticas firmes de un lado y compromiso desde el otro.

Igualmente, un punto sumamente fundamental que marcará la diferencia entre esa delgada línea es el fomento y proyección de una adecuada y correcta (en tiempo y forma) alfabetización digital[27] para alcanzar un uso responsable y positivo de las nuevas tecnologías. Es necesario que las empresas puedan aprender a convivir con las TIC, a sacarles el mayor provecho posible a las mismas y a educar a sus trabajadores en el modo correcto de usarlas[28].

Es así que en adición a lo anterior, y en palabras de Susana Rodríguez Escanciano, podemos aclarar que, "la experiencia demuestra, empero, cómo el poder tecnológico del empresario pone en peligro y moviliza numerosas libertades públicas, tales como el derecho a la intimidad, el secreto de las comunicaciones, el derecho a la propia imagen o la libertad informática"[29], en este sentido, nos atrevemos a sumar a la lista el derecho a la desconexión digital.

No obstante, por lo que se refiere al ordenamiento jurídico español, hemos apreciado que las TICs no han generado un impacto que haya tenido en general una traducción directa en la

[26] CALLE, Vicente. BYOD, "utiliza tu dispositivo personal para trabajar", la nueva revolución. cit.

[27] La alfabetización digital es un proceso de enseñanza y aprendizaje donde las personas son capaces de desarrollar las habilidades necesarias para lograr hacer un uso adecuado y responsable de las nuevas tecnologías. Hoy en día, son muchas las empresas que invierten tiempo y dinero en un plan de alfabetización digital para sus trabajadores, siendo esta una excelente vía para evitar los riesgos que conlleva un uso indebido de las TICs.

[28] UNIVERSIA ESPAÑA. *El impacto laboral de las TIC en la productividad laboral* [en línea]. Disponible en: https://noticias.universia.es/practicas-empleo/noticia/2016/11/17/1146271/impacto-tic-productividad-laboral.html

[29] RODRÍGUEZ ESCANCIANO, Susana. Derechos laborales digitales: garantías e interrogantes. cit. p. 17.

aparición de nueva legislación[30], y esto se ve acometido por ejemplo con el auge de la tendencia BYOD.

Por tanto, más adelante podremos ver claramente como el legislador no ha logrado incorporar los instrumentos jurídicos suficientes y capaces para canalizar adecuadamente la nueva realidad productiva de este tipo de tendencias que son fruto de la aplicación de las TICs al mundo laboral[31], provocando así algunas lagunas regulatorias muy significativas para la materia.

[30] DEL REY GUANTER, Salvador. Relaciones laborales y nuevas tecnologías: reflexiones introductorias. cit. p. 4.

[31] GORDO GONZÁLEZ, Luis. El Derecho del Trabajo 2.0: la necesidad de actualizar el marco de las relaciones laborales a las nuevas tecnologías. cit. p. 171.

III. BYOD EN EL ÁMBITO LABORAL

En los capítulos anteriores hemos podido esclarecer un panorama de cómo el ámbito laboral se ve rodeado, afectado y a la vez impulsado con el auge e incursión de las TICs.

Por tanto, en este apartado, podremos dilucidar como la proliferación de nuevas tecnologías, como las conexiones inalámbricas y dispositivos móviles, han impactado de manera muy significativa en la forma de trabajar de las empresas y sus trabajadores, permitiendo como característica principal a este hecho, la ubicuidad del trabajo, es decir, trabajar desde cualquier lugar, o la llamada movilidad que hemos expresado en el capítulo que precede[32].

Asimismo, podremos ver que cada vez es más frecuente que las empresas se apoyen en este tipo de tecnologías para facilitar y promover el acceso a la información y a los recursos corporativos en múltiples situaciones, sin perder de vista el conjunto de riesgos y amenazas inherentes a las mismas[33].

Cabe destacar, que gracias a esta movilidad, cada vez es mayor el número de trabajadores que utilizan la tecnología de la que son propietarios (hardware y software) para realizar tareas relacionadas con su trabajo[34]. Este fenómeno es denominado BYOD (*Bring Your Own Device* por sus siglas en ingles y *Trae tu propio dispositivo* en castellano) y procederemos a establecer una serie de fundamentos que nos ayuden a entender cuan complejo e importante puede ser su incorporación (explícita o implícita) en las empresas.

3.1 ¿Qué es BYOD?

El Centro Criptológico Nacional (en adelante, CCN), define el BYOD como "[…] la posibilidad de que los empleados de una organización usen los dispositivos de los que son

[32] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario* [en línea]. 2017, pág. 3. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

[33] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Op. cit. p. 3.

[34] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). *Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD)* [en línea]. 2013, pág. 4. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html

propietarios para desarrollar sus funciones profesionales, accediendo al entorno, servicios y datos corporativos" [35].

Mientras tanto que, el Instituto Nacional de Ciberseguridad (en adelante, INCIBE), expresa que el BYOD es un modo de trabajar que "[…] se caracteriza por el hecho de permitir a los empleados la incorporación de sus dispositivos móviles personales (portátiles, smartphones, tabletas) a las redes corporativas desde su casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales de los empleados" [36].

Con una adecuada bifurcación de los dos conceptos anteriores, podremos llegar a acotar tres pilares fundamentales que han de relucir para un idóneo entendimiento de esta tendencia y por consiguiente, para el posterior desarrollo y enfoque que se le dará al tema, enlazado con los beneficios y dificultades que esta arraiga hoy en día para las empresas y para el derecho laboral (en nuestro caso, el derecho laboral español).

Estos tres pilares son que el BYOD es y/o permite: 1) el uso de los dispositivos móviles de los empleados para uso laboral, 2) la conexión a recursos de la empresa (servicios y/o productos) y disponibilidad de la información empresarial en cualquier lugar y hora, y 3) el uso compartido de los dispositivos para fines laborales y personales.

Sentando base en los aspectos anteriores, la principal intención es la de dar a conocer que el BYOD no es simplemente tomar la decisión de llegar un día a nuestro lugar de trabajo y emplear nuestro dispositivo móvil personal para hacer un uso laboral del mismo, sin pensar que esto no conllevará una serie de matices (los cuales se irán desarrollando a lo largo del trabajo) que el empleador y el trabajador deberán conocer y tomar en cuenta para un apropiado uso e implementación de esta tendencia.

[35] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 5.

[36] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario. cit. p. 3.

3.2 Auge de la tendencia: un fenómeno en expansión

Tomando como punto de partida los conceptos previos, conviene puntualizar que no hay referencia exacta de la primera vez que la técnica ha sido mencionada, no obstante, su desarrollo se inició en el año 2009 en el seno de la compañía Intel que permitió y promovió esta política entre sus trabajadores[37].

Esto último, nos conlleva a poner sobre la mesa, que fue en los Estados Unidos, el país donde esta tendencia tiene su auge, marcando desde entonces una expansión sin precedentes donde cada vez, más empresas estuvieron aceptando, implementado y adaptando el BYOD para extraer la máxima utilidad del mismo.

Por lo tanto, no sería apropiado decir que esta tendencia se ha limitado exclusivamente a territorio americano, puesto que la realidad es que día a día son más las empresas de diferentes regiones que la adoptan.

En consecuencia, a lo largo de los últimos años han sido muchas las empresas o grupos de investigación que se han dado a la tarea de realizar un estudio donde se refleje cuantitativamente el impacto que el BYOD tiene hoy en día más allá de las fronteras estadounidenses.

Tal es el caso del grupo *Internet Business Solutions Group* de Cisco, donde en el año 2012 "amplió su estudio original sobre BYOD y virtualización para incluir a responsables técnicos tanto de grandes corporaciones (1000 empleados o más) como de empresas de tamaño medio (500-999 empleados) en ocho países de tres regiones", demostrando así, que el crecimiento del BYOD no se limita a los Estados Unidos, ni a las grandes empresas[38].

---

[37] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. p. 7.

[38] BRADLEY, Joseph; LOUCKS, Jeff; MACAULAY, James; MEDCALF, Richard y BUCKALEW, Lauren. *BYOD: una perspectiva global. Impulsar la innovación liderada por los empleados* [en línea]. 2012, pág. 1. Disponible en: https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons-Global_ES.pdf

A su vez, Gartner mediante un informe realizado por su analista David Willis en el año 2013, apuntaba que para el 2017, la mitad de las empresas implementarían la tendencia BYOD y ya no proporcionarían dispositivos tecnológicos a sus empleados. Esto debido a entre otras cosas, a que el trabajador se siente mucho más satisfecho y familiarizado realizando sus labores haciendo uso de su propia tecnología, que la provista por el mismo empresario. Asimismo, el informe continúa destacando que la tasa de adopción del BYOD en Estados Unidos. es el doble que la de Europa, pero la tasa más alta se encuentra en India, China y Brasil[39].

De igual manera, Lilach Bullock, columnista de Forbes, en el año 2019 ha destacado que el número de personas que incorporan sus dispositivos personales en su vida profesional a aumentado constantemente desde la llegada de los teléfonos inteligentes, computadoras portátiles y tabletas. Añadiendo que según estadísticos de la compañía Dell, el 50% de trabajadores de más de 30 años creen que las herramientas tecnológicas que usan en sus vidas personales son mucho más efectivas y productivas que las que usan en su vida laboral[40].

¿Y que más nos seguirá deparando el BYOD en el futuro? Aunque suene abrumador, esta tendencia a mutado a lo largo de los años y ahora nos encontramos con diferentes variaciones de la misma (las cuales no son primordiales para la realización de este trabajo), como ser el *Bring Your Own Application* (BYOA, por sus siglas en inglés, *Trae Tu Propia Aplicación* en castellano), en donde el trabajador no solo lleva su dispositivo personal al trabajo, si no que también hace uso de diferentes aplicaciones que lo ayuden a realizar sus tareas. Esto conlleva como principal problema, la seguridad de la aplicación descargada e instalada y como eso podría llegar a repercutir en riesgos tangibles para la empresa.

Igualmente, esta quedando en evidencia que a medida que la tecnología y las mejoras que estas brindan al aumento de capacidades físicas y cognitivas del humano (como ser dispositivos de realidad virtual), las empresas hoy en día están encontrando formas de

[39] KARANACUS, Chris. *Half of Companies Will Require BYOD By 2017, Gartner Says* [en línea]. Disponible en: https://www.cio.com/article/2386248/half-of-companies-will-require-byod-by-2017--gartner-says.html

[40] BULLOCK, Lilach. *The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future* [en línea]. Disponible en: https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/

aprovechar este tipo de tecnologías al mismo tiempo que mantienen la seguridad de sus recursos empresariales. Los expertos de Gartner sugieren que esto consistirá en gran medida en un acto de equilibrio entre mantener cierto control sobre estos dispositivos y al mismo tiempo permitir que los trabajadores los usen y que la empresa aproveche los beneficios que estos brindan[41].

Idealmente, lo anterior se conoce como *Bring Your Own Enhancement* (BYOE por sus siglas en ingles, *Trae Tu Propia Mejora* en castellano). Una tendencia que aún no tiene su pico en la industria, pero que según Gartner para el año 2023, el 30% de las empresas de TI entenderán sobre ellos, extendiendo así las políticas de BYOD a BYOE[42].

En adición a la anterior, y sin precedente alguno, hoy en día, una manifestación más del BYOD nace con el surgimiento de la pandemia por COVID-19. Nos referimos al «teletrabajo», modalidad de trabajo que ha sido el imprescindible amigo de las empresas para continuar la actividad de su negocio de una manera remota (o también llamada, a distancia).

Esta nueva forma de trabajar, facilita la operatividad diaria de la empresa, permitiendo que los empleados puedan acceder a los diferentes recursos de la misma desde el uso de dispositivos móviles, muchos de los cuales, los trabajadores son los propietarios, ocasionando así, que las empresas se vean obligadas a pasar al régimen del teletrabajo (siempre y cuando esto sea posible para ellas).

Este cambio improvisado de trabajo presencial a trabajo remoto, ha conllevado que en la mayor parte de los casos, los trabajadores aporten sus propios dispositivos, lo cual no se encuentra aún regulado, pero si hacemos un acercamiento al Real Decreto Ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19[43], su art. 5 nos hace referencia al carácter preferente del trabajo a

---

[41] WATTS, Stephen. *Why Bring Your Own Enhancement (BYOE) Is Trending in 2020* [en línea]. Disponible en: https://www.bmc.com/blogs/bring-your-own-enhancement-byoe/

[42] PANETTA, Kasey. *Gartner Top Strategic Predictions for 2020 and Beyond* [en línea]. Disponible en: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2020-and-beyond/

[43] Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3824

distancia, detallando que, "[…] se establecerán sistemas de organización que permitan mantener la actividad por mecanismos alternativos, particularmente por medio del trabajo a distancia, debiendo la empresa adoptar las medidas oportunas si ello es técnica y razonablemente posible y si el esfuerzo de adaptación necesario resulta proporcionado. Estas medidas alternativas, particularmente el trabajo a distancia, deberán ser prioritarias frente a la cesación temporal o reducción de la actividad."

Es así que constatamos que el BYOD seguirá tomando cada vez más un papel protagónico en las empresas, ya sea por situaciones convencionales en las que por ejemplo el trabajador quiera y decida usar sus propios dispositivos móviles para fines laborales durante la jornada de trabajo, o en situaciones excepcionales como la mencionada por COVID-19. Sin duda alguna, el BYOD seguirá teniendo un rol transcendental en las relaciones laborales.

3.3 Luces y sombras del BYOD

La implementación del BYOD conlleva a una serie de oportunidades y riesgos que los empleadores y los trabajadores deben conocer para realizar una adecuada adopción de la tendencia y de esa manera extraer la mayor utilidad de la misma. En los próximos escenarios, buscaremos definir como principal hecho las oportunidades que brinda el BYOD y su contra parte como riesgo. Entre ellos se pueden señalar los siguientes:

- ↑ **Flexibilidad del trabajo:** el uso de dispositivos móviles personales permite al trabajador un mayor sentido de comodidad, lo que a su vez conlleva una mejora en las condiciones de trabajo en las que se desenvuelve, promoviendo así el fomento de una buena flexibilidad laboral en el desarrollo de sus tareas.

- ↓ **Perdida del dispositivo:** siendo este uno de los mayores riesgos inherentes al uso de dispositivos móviles personales, ya que el trabajador además de conseguir una perdida material de su dispositivo, para la empresa conllevaría a una pérdida de información sumamente importante y confidencial.

↑ **Ahorro de costes:** esta oportunidad es claramente a beneficio del empleador, ya que al no proveer al trabajador de las diferentes herramientas de hardware y software para la realización del trabajo, se ahorra costos por la adquisición de esas tecnologías.

↓ **Gastos adicionales:** un entorno BYOD conlleva una serie de gastos e inversiones adicionales de gestión, mantenimiento, soporte e integración en los entornos TIC de las empresas, que normalmente no es tenido en cuenta, ya que muchas veces el BYOD se implementa de manera desapercibida en las mismas[44].

↑ **Mayor productividad:** el trabajador se siente mucho más cómodo y productivo al usar herramientas de alta capacidad y de las cuales ya tienen una alta comodidad en su interacción con las mismas, generando así una mayor satisfacción al momento de realizar sus tareas.

↓ **Alta distracción:** al hacer uso de sus propios dispositivos, el trabajador tiene al alcance de la mano diferentes distracciones de ocio (servicios de streaming, mensajería instantánea, aplicaciones multimedia, redes sociales, etc.) Siendo todo lo anterior un impedimento en la productividad esperada y deseada por parte del empleador.

3.4 Amenazas del BYOD sobre la seguridad de la información

Como ha sido mencionado en apartados anteriores, es sumamente importante delimitar que la información es el activo más importante en las empresas y la misma debe de poder ser manejada y resguardada en un entorno donde se mantenga su confidencialidad, integridad y disponibilidad. Siendo estos tres aspectos los cimientos bajo los que se construye la seguridad de la información, un concepto que abarca el conjunto de medidas preventivas y correctivas que las empresas deben tener en cuenta al hacer uso de las TICs.

[44] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. p. 8.

Hoy en día existen numerosas amenazas y vulnerabilidades asociadas al BYOD que pueden poner en riesgo la seguridad, tanto del dispositivo, como de la información que gestionan y los recursos corporativos a los que se accede[45].

Ante tales escenarios, conviene tener en cuenta que más de un tercio de las vulnerabilidades podría derivar potencialmente en una violación completa de los aspectos de seguridad antes mencionados: hacer que el sistema completo quede fuera de servicio (ataque a la disponibilidad), realizar alteraciones en los ficheros del sistema (ataque a la integridad), acceder a los ficheros del sistema (ataque a la confidencialidad), y además, suplantar la identidad del usuario del dispositivo (autenticación)[46].

Por todo ello, las empresas deben realizar periódicamente análisis de amenazas ante este tipo de vulnerabilidades. A continuación, se brinda una serie de amenazas y/o vulnerabilidades asociados al uso del BYOD en las empresas:

- **Dispositivos desactualizados:** cuando un dispositivo no cuenta con la última versión de sistema operativo y/o aplicaciones, o todos los parches de seguridad necesarios y recomendados por los fabricantes de dichos softwares, se vuelven vulnerables ante fallos de seguridad que sean conocidos por ciber atacantes[47].

- **Uso de aplicaciones o contenidos no confiables:** los dispositivos propiedad de los trabajadores presentan importantes deficiencias en materia de seguridad derivadas tanto de su propia estructura como de un uso inseguro[48]. La instalación de aplicaciones de terceros, sin saber aspectos de seguridad de las mismas, ponen en alto riesgo los dispositivos y la información que estos almacenan.

---

[45] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 10.

[46] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 10.

[47] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Bondades y riesgos del BYOD* [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/bondades-y-riesgos-del-byod

[48] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. p. 12.

- **Conexiones inalámbricas inseguras:** hacer uso de redes inalámbricas públicas (cafeterías, aeropuertos, hospitales, hoteles, entre otros) permitirá a los ciber atacantes conseguir acceder al dispositivo y robar la información perteneciente al trabajador. Por lo que, almacenar información corporativa en estos dispositivos es un alto riesgo para la empresa, ya que el empleador no tiene poder de control sobre el uso que los propietarios hagan de los mismos.

- **Interconexión con otros sistemas:** las interconexiones más usuales son aquellas que tienen lugar, a través de mecanismos inalámbricos o por cable, entre el dispositivo móvil y una computadora de escritorio o portátil, con el objetivo de sincronizar el contenido de ambos equipos. Ejemplos de estos riesgos se dan cuando se conecta un dispositivo móvil de titularidad del trabajador a una computadora de titularidad de la empresa[49].

- **Uso de servicios de geolocalización:** aquellos dispositivos móviles que mantienen activos los servicios de geolocalización suponen un riesgo adicional, ya que se le posibilita al ciber atacante determinar la posición del trabajador en función de la localización de su dispositivo móvil, lo que puede afectar gravemente no sólo a la seguridad de la empresa, sino también a las garantías de privacidad del propio trabajador, facilitando la creación de mapas geográficos de los movimientos físicos de los mismos y, en algunos casos, el tipo de actividad que desarrollan[50].

- **Trabajadores que han terminado su relación laboral**: si la relación laboral termina en malos términos, el trabajador al ser el propietario del dispositivo, puede que descargue en el información confidencial para posteriormente hacer un uso inadecuado de ella. En esta vulnerabilidad entra en juego el aspecto de la confidencialidad de la información.

[49] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 14.

[50] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 15.

- **Aspectos legales:** a lo largo de este trabajo, veremos como la implementación del BYOD acarrea consigo una serie de aspectos legales importantes y notorios para el empleador y el trabajador. Desde la perspectiva del estatuto de los trabajadores ante tales situaciones, pasando por los derechos fundamentales, laborales digitales, la normativa de protección de datos y los convenios colectivos. Cabe destacar que una incorrecta implementación y posterior monitorización de esta tendencia, puede vulnerar derechos de los trabajadores que podrían desencadenar procesos judiciales en contra de las empresas.

3.5 BYOD, ¿privilegio o necesidad?

Ante toda la serie de matices detallados previamente con respecto al uso del BYOD, nos surge la duda de que si hoy en día el mismo debe ser considerada un privilegio o una necesidad dentro de las empresas, y no orientándolo indiscriminadamente solo por parte del empleador o del trabajador, si no que considerándolo desde ambas perspectivas, desde su parte como una oportunidad que hay que aprovechar, hasta su parte como un riesgo que se debe tener en cuenta y poseer los controles necesarios para mitigarlos.

Desde la perspectiva del trabajador, el principal impulsor del BYOD es la capacidad de poder acceder a sus aplicaciones preferidas en cualquier momento**,** sobre todo a las redes sociales y comunicaciones privadas. La dependencia de las comunicaciones personales es muy importante, por lo que bajo este escenario, la tendencia se convierte en un privilegio[51].

En su contraparte, bien es cierto que en muchas ocasiones, los empleadores no siempre dotan a sus trabajadores con las mejores condiciones tecnológicas para el desarrollo de sus tareas, por consiguiente, el trabajador se ve en la necesidad de usar sus propios dispositivos, en pro de satisfacer sus exigencias tecnológicas.

[51] ROJAS, Elisabeth. *El BYOD, ¿un privilegio o un derecho?* [en línea]. Disponible en: https://www.muycomputerpro.com/2012/06/19/byod-privilegio-derecho

Por parte del empleador, la implementación del BYOD se vuelve un privilegio cuando este se desliga de propiciar al trabajador las herramientas tecnológicas, ya que es el mismo trabajador quien las aporta.

Sin embargo, el BYOD por parte del empleador se vuelve una necesidad cuando este se integra con la empresa, promoviendo así que la misma realice los mecanismos necesarios para incorporarla correctamente y de esa manera, lograr un entorno laboral acoplado con el buen uso de las TICs, en concordancia con los intereses de la empresa y con la no vulneración de los derechos fundamentales y laborales digitales de los trabajadores.

IV. RIESGOS JURÍDICO-LABORALES DEL BYOD

En la actualidad no existen normas específicas que regulen la utilización del BYOD en el ámbito empresarial, por lo que su configuración jurídica debe extraerse a partir de un conjunto de disposiciones que regulan la privacidad, las relaciones jurídicas en los centros de trabajo, los derechos fundamentales, los derechos laborales digitales, la propia normativa laboral general, como también de un conjunto unificado de jurisprudencia que aunque no sea fuente del derecho y no trate específicamente sobre la solución de problemas relativos al tema aquí analizado, nos ayudará a definir ciertos caminos interpretativos para acercarnos a un ideal regulativo del mismo[52].

En palabras de Oriol Cremades Chueca, "el «propietarismo» ha venido siendo la visión imperante que los tribunales españoles han adoptado para el análisis jurídico-laboral de las nuevas tecnologías, pero la utilización de dispositivos móviles personales para fines profesionales (BYOD), rompe este paradigma"[53].

Ante tal apreciación de dicha visión propietarista, cabe destacar que la iniciación de esta data del 26 de septiembre de 2007, cuando el Tribunal Supremo afirmaba que: "las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario «como propietario o por otro título» y este tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen"[54].

Por lo tanto, es a partir de ese momento, cuando la mayoría de la jurisprudencia española ha hecho alusión al carácter propietarista y al poder de control que los empleadores poseen sobre los dispositivos tecnológicos que los mismos ponen a disposición de los trabajadores.

---

[52] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 117.

[53] CREMADES CHUECA, Oriol. "Impacto teórico-práctico del BYOD en el derecho del trabajo". *Revista de Trabajo y Seguridad Social* [en línea]. 2018, núm. 2018, pág. 103. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6470608

[54] STS de 17 de diciembre de 2007 (rec. 966/2006).

Sin embargo, lo anterior ha generado que con el uso de nuevas tecnologías o tendencias tecnológicas, como es el caso del BYOD, y los cambios que eso acarrea en la operatividad del trabajo, se presenten algunos conflictos jurídico-laborales que acarrean un reto al legislador a la hora de regular sobre este tópico, existiendo hoy en dia una serie de normativa vigente que no se ajusta a la realidad a la que se enfrentan los empleadores y trabajadores, mostrando severas lagunas o carencias.

Por ello es que, de no contarse con una regulación acorde, nos enfrentamos ante una posible vulneración (difícil de resolver) de derechos fundamentales como el de la intimidad, a la propia imagen, al secreto de las comunicaciones o la protección de datos de carácter personal, como también a los derechos digitales con los que cuentan los trabajadores, por ejemplo el derecho a la desconexión digital.

Por tal razón, en las páginas siguientes, se analizará si, ante la inexistencia de una normativa específica sobre el uso para fines profesionales que los trabajadores hacen de los dispositivos móviles de los cuales ellos son propietarios, es necesario proceder a la introducción de una ordenación específica en nuestro ordenamiento jurídico o, por lo menos, debe ser una materia de atención prioritaria por los interlocutores sociales.

4.1 Aproximación al Estatuto de los Trabajadores

Tal y como se apuntó supra, hemos podido observar que una de las cuestiones de más actualidad en el derecho laboral es la referida al alcance de control empresarial sobre la actividad de los trabajadores cuando estos utilizan las tecnologías que son puestas a su disposición por parte del empleador.

Y es bajo esa precisa acción cuando se abre la brecha que genera una colisión de ese control con los derechos fundamentales y laborales digitales anteriormente mencionados[55], pero ¿qué pasa si las tecnologías son propiedad del trabajador?, ¿podría el empleador en igual medida

[55] GONZÁLEZ GONZÁLEZ, Carlos. "Control empresarial de la actividad laboral y uso de las nuevas tecnologías". *Revista Aranzadi Doctrinal* [en línea]. 2015, núm. 11, pág. 128. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5319216

seguir ejerciendo su capacidad de control de la actividad laboral sobre el uso de esas tecnologías?

Si hacemos un recorrido por el ET, encontramos en su art. 20 una clara referencia a la dirección y control de la actividad laboral. Su apartado primero nos especifica que "el trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue". Adicionando en su apartado tercero que "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".

Por consiguiente, de no respetarse las garantías adecuadas, lo anterior puede llegar a ocasionar la vulneración de derechos fundamentales de los trabajadores, dejando entre ver que el empresario no solo por ser la parte con más poder de la relación laboral, puede ejercer sus capacidades de control por encima del respeto de esos derechos correspondientes a los trabajadores. Y esto, sin aún llegar a diferenciar si el trabajador es el dueño o no de los dispositivos tecnológicos con los que ejerce sus labores.

Lo que si es cierto, es que los medios o instrumentos que la empresa pone a disposición de los empleados no pueden ser utilizados para uso personal si ello no está expresamente autorizado, pues supondría una transgresión de la buena fe contractual y a su vez daría paso a una causa de despido disciplinario. Para contrarrestar eso, se debe establecer un obligado deber de información por parte de los empleadores a los trabajadores sobre los criterios de uso de los dispositivos tecnológicos en la empresa[56].

Por lo tanto, será necesario poder determinar cuándo el control empresarial es de legítimo interés por parte del empleador y es respetuoso con los derechos imbricados. Y es así como sobre este aspecto han tenido ocasión de pronunciarse los tribunales, pero las respuestas no han sido siempre iguales y la valoración judicial depende muchas veces del contexto de la

[56] QUÍLEZ MORENO, José Mª. "La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores". *Revista Española de Derecho del Trabajo* [en línea]. 2019, núm. 217, págs. 131 y ss. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7029834

situación y del concreto medio tecnológico que ha sido controlado por la empresa en relación con el derecho fundamental o laboral digital que esté implicado en cada caso[57].

En consecuencia, la doctrina del Máximo Intérprete de la Constitución en España nos brinda una serie de pronunciaciones que nos ayudan a sentar base en esta disyuntiva. En la Sentencia del Tribunal Constitucional 213/2002[58], de 11 de noviembre, se destaca la necesidad de que "los órganos judiciales preserven el necesario equilibrio entre las obligaciones del trabajador dimanantes del contrato de trabajo y el ámbito de sus derechos y libertades constitucionales".

De igual manera, diez años después, la Sentencia del Tribunal Constitucional 241/2012 nos muestra una clara referencia sobre la variabilidad de las medidas de vigilancia y control del empleador sobre los medios informáticos, exponiendo que "los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin".

En este sentido, podemos evidenciar que el art. 20 del ET, aquilatado en sus términos, es el medio normativo por el que se permite al empleador aplicar su actividad de control a los recursos TIC corporativos utilizados por sus trabajadores, pero habrá que ser muy prudentes en la extensión de este control a los dispositivos que son propiedad de los trabajadores. La capacidad de control del empleador deberá quedar limitada exclusivamente a las áreas, aplicaciones y contenedores de información corporativa, sin perjuicio del posible análisis forense de todo el contenido del dispositivo en el seno de una investigación judicial, o con el consentimiento del usuario[59].

Esta capacidad de control a la que hacemos alusión y la que ahora deberá quedar limitada por el auge de tendencias como el BYOD, abre camino para discernir que por desgracia y como

[57] GONZÁLEZ GONZÁLEZ, Carlos. Control empresarial de la actividad laboral y uso de las nuevas tecnologías. cit. p. 112.

[58] STCo 213/2002, de 11 de noviembre.

[59] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 63.

ya se contemplaba, la tecnología siempre va un paso más adelante que el derecho, mostrando que sin duda alguna, la normativa existente no cumple con las garantías necesarias para proteger al trabajador ante cualquier vulneración de sus derechos mediante un control o vigilancia indebido de sus propios dispositivos por parte del empleador.

Sin embargo, el legislador en su convicción de querer establecer todos los medios de protección necesarios para que en este caso los trabajadores hagan valer y respetar sus derechos, introduce reformas a la normativa existente. Y es así como precisamente en la Disposición Final 13ª de la LOPDyGDD, se introduce un nuevo artículo en el ET, denominado art. 20 bis[60], y lo hace remarcando, tras el reconocimiento del poder de dirección y control de la actividad laboral por parte del empleador en el art. 20 (ya antes referenciado), la importancia que tiene la intimidad de los trabajadores sobre el control que el empleador puede ejercer en el nuevo y creciente entorno digital y de las nuevas (o ya no tan nuevas) tecnologías[61].

Lo anterior, es un inicio sumamente importante para tener en consideración que con el auge de nuevas tecnologías o tendencias tecnológicas como el BYOD, los trabajadores están expuestos a un entorno digital, que como hemos visto con antelación, altera las relaciones labores convencionales, dando paso a que estos puedan exigir cada vez más el respeto a su intimidad y demás derechos que les pertenecen cuando los mismos hagan uso de nuevas tecnologías.

No obstante, aunque este sea un gran comienzo al acercamiento de un precepto normativo que nos aproxime a regular una de las realidades laborales a las que hoy en día se enfrenten tanto el empleador como el trabajador, la realidad es que no podemos dar nada por sentado e interpretar la norma a conveniencia, ya que la misma carece de explicitud al momento de considerar el respeto de dichos derechos frente al uso de dispositivos móviles que son

[60] Estatuto de los Trabajadores. Artículo 20 bis. *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión:* Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

[61] QUÍLEZ MORENO, José Mª. La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores". cit. p. 129.

propiedad de los trabajadores. Además, al ser un artículo bis, este debe de interpretarse armónicamente con el artículo que le precede.

Asimismo, es muy oportuno observar como el legislador queriendo buscar una solución a la no vulneración de derechos atañables a los empleados, hace gran alusión y cuidado al respeto a la intimidad de los mismos con relación al entorno digital, introduciendo de igual manera, un novedoso concepto denominado "desconexión digital", el cual estaremos desarrollando más adelante en este trabajo.

Es así que, con los diferentes acercamientos que daremos del BYOD al ordenamiento jurídico español, al final de este capítulo estaremos brindando una serie de pautas con las cuales se esta proponiendo y logrando regular esta tendencia, que como vimos en apartados anteriores, vino para quedarse.

4.2 Impacto en los derechos fundamentales y laborales digitales

Los derechos fundamentales y laborales digitales de los trabajadores deben hacer frente desde hace unos años a la potencialidad invasiva de las nuevas tecnologías aplicadas al ejercicio del poder empresarial, de forma que el derecho a la intimidad, al secreto de las comunicaciones, a la propia imagen, a la desconexión digital y a la protección de datos de carácter personal se ven limitados por formas de control empresarial imprevisibles hace tan sólo una década[62].

Es por eso que como se ha evidenciado hasta este momento respecto de la tendencia del BYOD, existe una laguna normativa y carencia jurisprudencial al respecto, por ello las consecuencias legales derivadas de su implantación deben extraerse por analogía de las

[62] SÁEZ LARA, Carmen. "Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y las comunicaciones". *Temas Laborales: Revista andaluza de trabajo y bienestar social* [en línea]. 2017, núm. 138, pág. 186. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6552393

normas actualmente existentes en materia de derechos fundamentales, y las que protegen las relaciones de índole laboral[63].

En este apartado, analizaremos, si bien brevemente, una serie de derechos fundamentales y laborales digitales implicados que son recogidos en primera instancia por la Constitución Española de 1978 (en adelante, CE) en su art. 18 (apartados 1, 3 y 4), como de igual manera en la LOPDyGDD, con el fin de dilucidar si se puede extender la aplicación de los mismos a la tendencia en estudio, que problemáticas acarrea ello, y la necesidad o no de una regulación nueva o actualizada.

4.2.1 Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral

En palabras de Javier Puyol, "la intimidad es el derecho que poseen las personas de poder excluir a las demás del conocimiento de su vida privada, es decir, de sus sentimientos y comportamientos […]. El derecho a la intimidad consiste en una especie de barrera o cerca que defiende la autonomía del individuo humano frente a los demás y, sobre todo, frente a las posibles injerencias indebidas de los poderes públicos, sus órganos y sus agentes"[64].

Entre los distintos bienes de la personalidad que la CE[65] contempla, es en el art. 18, apartado 1, donde se extiende la protección a la esfera de la libertad individual, a través de un sistema de garantías en torno a la vida privada de las personas, que permite ejercer un control material sobre el tratamiento de su información personal[66]. Dicho art. 18.1 nos dice que: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Y cabe destacar que tal y como se pone de manifiesto en la Sentencia del Tribunal Constitucional 134/1999[67], "el artículo 18.1 no garantiza una "intimidad" determinada […].

---

[63] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 117.

[64] PUYOL, Javier. Op. cit. p. 132.

[65] Constitución Española, de 29 de diciembre de 1978. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[66] ORDOÑEZ PASCUA, Natalia. Relaciones de trabajo y ciberseguridad: nuevos retos en un futuro tecnológico incierto. cit. p. 251.

[67] STCo 134/1999, de 15 de julio. FJ 5.

Lo que el artículo 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio".

Bajo el panorama descrito y por cuanto al aspecto normativo hace, la protección de la intimidad de los trabajadores cuenta con un garante complementario en la norma laboral que a lo largo de su articulado da muestra del derecho cualificado de los trabajadores a disponer de su intimidad respecto al empleador[68]. En tal sentido, el art. 4, apartado 2, inciso e) del ET dispone que "en la relación de trabajo, los trabajadores tienen derecho al respeto de su intimidad y a la consideración debida a su dignidad".

Asimismo, algo novedoso sucede en el contexto del Título X de la LOPDyGDD, donde el legislador asumiendo de momento la necesidad de abordar el reto de un debido reconocimiento a un sistema de garantía de derechos digitales concernientes a los trabajadores[69], establece el art. 87 sobre el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral[70]. Siendo este una pauta tanto para el trabajador, como para el empleador, sin dejar de lado que aún así sigue existiendo como se verá a continuación una laguna regulatoria ante la tendencia del BYOD.

Hasta este punto, lo que si debemos evidenciar es que la mayoría de escenarios en los que se ve vulnerado el derecho a la intimidad de los trabajadores, es cuando los mismos hacen un uso personal de los dispositivos tecnológicos que el empleador pone a su disposición[71], ya que este último aún se encuentra facultado por el art. 20.3 del ET y ahora por el art. 87.2 de

[68] ORDOÑEZ PASCUA, Natalia. Relaciones de trabajo y ciberseguridad: nuevos retos en un futuro tecnológico incierto. cit. p. 254.

[69] BAZ RODRIGUEZ, Jesús. Privacidad y protección de datos de los trabajadores en el entorno digital. cit. págs. 145 y ss.

[70] Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Artículo 87.1**.** *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral:* Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

[71] SÁEZ LARA, Carmen. Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y las comunicaciones. cit. págs. 209 y ss.

la LOPDyGDD para poder ejercer su poder de control y vigilancia sobre la actividad laboral de los trabajadores y por consiguiente del uso que los mismos hagan con los dispositivos tecnológicos de los cuales la empresa es propietaria.

Como pone de relieve el Tribunal Supremo, estos conflictos surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa.[72]. Sin embargo, en cualquier caso, el art. 87.3 e *in fine* de la LOPDyGDD establece claramente que el empresario a tenor de prever algunos conflictos de esta índole, debe especificar y comunicar a los trabajadores de manera precisa "los usos autorizados", de forma que en primera instancia el trabajador conozca el uso que le puede dar a dichos dispositivos y en segunda, que el empleador conozca hasta dónde puede llegar su poder de control a la hora de acceder a los dispositivos tecnológicos utilizados por sus trabajadores[73], impidiendo así que se generen conflictos entre ambas partes.

Bajo tales circunstancias, "lo difícil es distinguir, la esfera privada de la pública de cada trabajador en el ámbito laboral, además de conocer la situación de cada empleado y su contrato de trabajo. Ya que en muchos casos, los empresarios informan a sus trabajadores del uso que deben hacer de sus equipos informáticos, y si estos, deben dedicarse exclusivamente al ámbito laboral y, por tanto, podrán ser revisados por el empresario"[74], ¿pero y que pasa con los dispositivos móviles que son propiedad de los trabajadores?, ¿El empleador tendrá el mismo alcance de control que le habilita la ley?

Ante la implementación del BYOD en la empresa y siendo el empleador consciente de ello, el precepto normativo que más nos puede acercar a una regulación del mismo (aunque no es meramente acertado para la materia, dado que quedan muchos aspectos que no se toman en cuenta para una regulación idónea y certera de la misma) es lo previsto en el art. 18 del ET[75],

---

[72] SÁEZ LARA, Carmen. Op. cit. p. 207.

[73] FERNÁNDEZ ORRICO, Fco. Javier. "Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre". *Revista Española de Derecho del Trabajo* [en línea]. 2019, núm. 222, pág. 47. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7059685

[74] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 144.

[75] Estatuto de los Trabajadores. Artículo 18. *Inviolabilidad de la persona del trabajador:* Solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la

donde el empleador podría llegar a realizar un control sobre el dispositivo móvil del cual el trabajador es propietario, atendiendo en ese punto a que el dispositivo es efecto personal del trabajador.

Lo anterior asegura que el empleador puede realizar un debido control basándose en el principio de proporcionalidad (es decir, no realizando intromisiones ilegítimas y extensivas a los datos, archivos y/o aplicativos corporativos que conciernen a la empresa) y existiendo un interés genuino y razonable por parte de él para poder realizarlo, pero sin pasar por alto las garantías necesarias del art. 18 del ET, las cuales como apunta Oriol Cremades Chueca "deberían ser aplicadas como principio general en el BYOD"[76], ya que de no hacerse, sería una clara e irreparable violación a la intimidad del trabajador.

Es así como deberemos de tener en cuenta que ante una posible vulneración del derecho a la intimidad dada la aplicación del BYOD, es necesario considerar una vertiente que es sumamente importante tener en mente, ya que al permitir (directa o indirectamente) a que el trabajador pueda hacer uso de sus propios dispositivos móviles, eso no es sinónimo de que el mismo queda exento a que el empleador siga ejerciendo su poder de control, aunque es cierto que este último ahora tiene que llevarlo a cabo con un deber de diligencia extremadamente cuidadoso y oportuno cuando lo realice.

Por ejemplo, con la información que hemos propiciado en el capítulo anterior, una de las realidades que denotan un carácter negativo de esta tendencia y a la que el empleador se enfrenta al momento en el que el trabajador hace uso de sus propios dispositivos, es que existe un mundo de distracciones completamente amplio y ajenos a la injerencia de la empresa, por lo que el trabajador puede pasar más tiempo en asuntos personales que en el desarrollo de su actividad laboral, ¿será lo anterior un indicio suficiente para que el empleador pueda ejercer su derecho de control?

---

protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

[76] CREMADES CHUECA, Oriol. Impacto teórico-práctico del BYOD en el derecho del trabajo. cit. p. 113.

Bajo ese contexto, por supuesto que el empleador puede ejercer tal derecho, primeramente por un incumplimiento disciplinario por parte del trabajador al no cumplir debidamente con su jornada de trabajo en tiempo y forma, y dos, por que a nivel del empleador existiría un interés legítimo por parte de él (sospecha de inactividad laboral durante la jornada de trabajo) habilitándose lo estipulado en el art. 20.3 del ET, como también del art. 87.2 de la LOPDyGDD.

Sin embargo, y en consecuencia a lo que hemos reparado en explicaciones anteriores, con el auge del BYOD se puede llegar a vulnerar gravemente la intimidad de los trabajadores si el empleador no tiene el reparo necesario al hacerlo, ya que el trabajador al ser el propietario del dispositivo, tiene un mayor grado de expectativa de intimidad ante su uso.

4.2.2 Derecho al secreto de las comunicaciones

Como señala Oriol Cremades Chueca, "al igual que el derecho a la intimidad, el secreto de las comunicaciones puede verse comprometido cuando el empleador ejerce su facultad de control y entendemos que deberían seguirse unas pautas con una lógica similar a las expuestas para el derecho a la intimidad"[77].

A lo que en materia de CE respecta, el derecho al secreto de las comunicaciones se encuentra recogido en el art. 18, apartado 3 de dicha constitución, afirmando que "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

Como podemos apreciar, el art. 18.3 CE menciona explícitamente las comunicaciones postales, telegráficas o telefónicas, pero no hay que excluir por ello otro tipo de comunicaciones, dado el carácter abierto de su enunciado. Por tanto, en la actualidad, entendemos que habría que incluir las comunicaciones efectuadas mediante correo electrónico, mensajería instantánea, entre otros, siempre y cuando se efectúen mediante algún

[77] CREMADES CHUECA, Oriol. Op. cit. p. 114.

dispositivo o artificio técnico[78] o cualquier otro tipo de canal, sistema o producto oficial que interponga la empresa para su uso en la jornada de trabajo.

Existe un criterio en la materia que considera requisito indispensable para que haya "comunicación" en los términos del artículo 18.3 CE, que exista una infraestructura o dispositivo comunicativo, que no tiene que ser sumamente sofisticado, pero que por tanto exija una distancia real entre los comunicantes. Asimismo, también se exige que la comunicación se realice por "canal cerrado", puesto que si la transmisión de la información o mensaje no se lleva a cabo de esa manera, en modo alguno hay que considerar si estamos o no ante la posibilidad de aplicar el derecho al secreto de las comunicaciones, ya que no habrá expectativa razonable de secreto[79].

¿A que nos referimos con "canal cerrado"? Hay que comenzar señalando que "el secreto de las comunicaciones constituye una garantía objetiva, que protege cualquier comunicación con independencia de su contenido, es decir, tanto si se trata de una comunicación referida a aspectos íntimos, como si tiene por objeto cualquier otra cuestión, aunque sea intrascendente"[80].

Es así que entenderemos por un canal cerrado, independientemente del contenido a tratar, a todo medio en el que se pueda efectuar una comunicación entre las partes involucradas en el proceso comunicativo, sin la intromisión no consentida de un tercero.

Así por ejemplo, el derecho al secreto de las comunicaciones se aplicará al correo electrónico, a las videoconferencias, al envío de mensajes a través de aplicativos de mensajería instantánea o a las comunicaciones telefónicas que tienen lugar en internet, mientras que, a

[78] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 146.

[79] PUYOL, Javier. Op. cit. p. 148.

[80] DÍAZ REVORIO, F. Javier. "El derecho fundamental al secreto de las comunicaciones". *Derecho PUCP: Revista de la Facultad de Derecho* [en línea]. 2006, núm. 59, pág. 162. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5085108

otras formas de comunicación que se realicen por canal abierto (tales como radio o chat entre varios interlocutores) no les será de aplicación la protección del artículo 18.3 CE[81].

Uno de los posibles escenarios en los que se puede vulnerar el derecho al secreto de las comunicaciones de los trabajadores, es a través del uso del correo electrónico corporativo, servicio propiedad de la empresa, el cual, es provisto al trabajador para la realización de sus actividades laborales. Lo anterior independientemente de si el dispositivo donde se está accediendo a dicho servicio es propiedad del empleador o del trabajador.

El mayor referente jurisprudencial en la materia, es el famoso caso Barbulescu II[82], recogido en la sentencia dictada por el Tribunal Europeo de Derechos Humanos (en adelante, TEDH), el 5 de septiembre de 2017, en la cual se delimitan los limitantes y factores de control que puede ejercer el empleador ante el uso de las nuevas tecnologías, como ser el correo electrónico.

La sentencia nos dice que "las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario", añadiendo que "debe hacerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o sólo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados".

A este punto, se debe mencionar que una realidad presente en las empresas es que un número considerable de trabajadores hace uso del correo electrónico corporativo para realizar comunicaciones extralaborales, generando así una falta disciplinaria muy grave que podría llegar a afectar la relación laboral.

Para poder lograr mitigar ese uso indebido, recomendablemente, el empleador deberá informar a sus trabajadores sobre el uso estrictamente laboral que se le debe dar al correo

[81] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 148.

[82] TEDH, Sentencia 5 de septiembre de 2017.

electrónico. Por consiguiente, en caso que si exista un uso indebido o alguna mínima sospecha del mismo por parte del empleador, esto último generaría un interés legítimo para que el empleador quiera revisar dichas comunicaciones.

Por tanto, ¿el empleador está o no facultado para intervenir los correos electrónicos de sus trabajadores? Sea o no un escenario donde tenga presencia el BYOD o más allá del interés legítimo que el empleador sostenga para llevar a cabo dicha intervención, son las referencias jurisprudenciales en materia las que introducen un nuevo criterio en cuanto al control empresarial del uso del correo electrónico, lo anterior en pro de proteger el secreto de las comunicaciones, abriendo así, una puerta a la necesidad de una autorización judicial para otorgar validez a las comunicaciones intervenidas[83].

Sin embargo, el poseer una autorización judicial no es sinónimo de tener absoluta potestad para revisar todos los correos electrónicos del trabajador. Es sumamente importante delimitar que el secreto de las comunicaciones en este ámbito, protegerá cualquier correo electrónico que el trabajador aún no hubiera tenido la oportunidad de abrir y/o leer.

Es así que con la autorización judicial se podrá hacer solo un control de los correos electrónicos ya abiertos y/o leídos por el trabajador. Tengamos en mente que de no hacerse así, no solo se vulnerarían derechos del trabajador, sino que también derechos de terceros que estén involucrados en la comunicación.

Asimismo es importante acotar que sin una autorización judicial pertinente y oportuna, la intervención del correo electrónico sería ilícita, dando paso a que esta no pueda ser considerada como prueba en caso de llevarse a cabo un proceso judicial, además de que desencadenaría una serie de problemas legales que el empleador deberá asumir al menoscabar de esa manera uno o más derechos fundamentales del trabajador.

Estrictamente, en los supuestos en el que el trabajador haga uso de sus propios dispositivos móviles para acceder al correo electrónico de la empresa, primeramente y sin entrar en tecnicismos, el empleador deberá asegurarse que esos dispositivos cuentan con todos los

[83] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. págs. 153 y ss.

requerimientos mínimos de seguridad para hacer uso de un servicio tan crítico y sensible como lo es el correo electrónico, ya que recordemos que en el se almacenan y fluyen comunicaciones con información de carácter sensible y confidencial.

Una vez aclarado ese punto, si al realizar una intervención del correo electrónico en un dispositivo móvil propiedad del trabajador no se tiene en cuenta una correcta diligencia para llevar a cabo la acción, y si la intervención se extralimita a cualquier otro ámbito que no sea el correo electrónico, se estaría llevando a cabo una intromisión ilegítima lesiva de varios derechos fundamentales.

Evidenciamos así, que con el BYOD, por más que el correo electrónico sea un servicio propiedad de la empresa, su posible control al estar en uso mediante un dispositivo personal del trabajador, tiene un conjunto de matices que deben ser considerados, como ser una posible vulneración de la intimidad y al secreto de las comunicaciones no solo del trabajador, sino también de terceros.

4.2.3 Derecho a la desconexión digital

Conforme a lo que hemos venido desarrollando, es de nuestro conocimiento que las TICs han hecho surgir nuevas formas en la organización del trabajo y con ellas nuevos problemas en relación con la delimitación entre tiempo de trabajo y descanso, produciendo ventajas tales como la libertad de trabajar fuera de la oficina, pero también inconvenientes que afectan, principalmente, a la esfera privada y de salud de los trabajadores (generando estrés, agotamiento, entre otros). El uso de las nuevas tecnologías y tendencias como el BYOD están cambiando no sólo nuestra manera de trabajar, sino que también son condicionantes de nuestro descanso[84].

Aunque en el ordenamiento jurídico español no figura un concepto claramente delimitado de lo que es la desconexión digital, es gracias a la relación de gestación y nacimiento en las

[84] PÉREZ CAMPOS, Ana Isabel. "La desconexión digital en España: ¿un nuevo derecho laboral?". *Anuario Jurídico y Económico Escurialense* [en línea]. 2019, núm. 52, pág. 104. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6883975

políticas de reforma del Gobierno Francés en el año 2017[85] que podemos discernir que este derecho se traduce en la acción de no estar conectado a ningún dispositivo digital que pueda ocasionarle una interrupción del tiempo extralaboral al trabajador, como puede ser el previsto para el descanso o la realización de cualquier otra actividad diferente, salvo, claro sean situaciones excepcionales de emergencia justificada[86].

Es así que, y a diferencia de otros países (como el ya mencionado Francia) no fue hasta la reciente aprobación de la LOPDyGDD, de protección de datos personales, cuando España expresa un tratamiento normativo específico sobre el derecho a la desconexión digital en el ámbito laboral, cerrando así una laguna jurídica que existía hasta el momento[87].

Si bien este derecho no tiene carácter de derecho fundamental, es entonces cuando el legislador establece en el art. 88, apartado 1 de dicha ley que "los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar".

De igual manera, es importante remarcar a tenor de lo anterior, que el citado precepto normativo llama a la negociación colectiva como vía para definir la mejor forma de ejercer el derecho (art. 88, apartado 2[88]), pero sólo otorga un derecho de audiencia a los representantes de los trabajadores en la definición de la política interna empresarial en relación a la desconexión, es decir, en la concreción de las modalidades de disfrute del derecho, las acciones de formación y sensibilización de personal sobre un uso razonable de

---

[85] NARANJO COLORADO, Luz Dary. "Vicisitudes del nuevo derecho a la desconexión digital: Un análisis desde la base del derecho laboral". *Revista Saber, Ciencia y Libertad* [en línea]. 2017, núm. 2, pág. 50. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6556861

[86] FERNÁNDEZ ORRICO, Fco. Javier. Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre. cit. p. 62.

[87] BARRIOS BAUDOR, Guillermo L. "El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones". *Revista Aranzadi Doctrinal* [en línea]. 2019, núm. 1, pág. 2. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6771678

[88] Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Artículo 88.2. *Derecho a la desconexión digital en el ámbito laboral:* Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

las herramientas tecnológicas, las formas para evitar el riesgo de fatiga informática o las medidas específicas para los teletrabajadores (art. 88, apartado 3)[89].

Sin embargo, veremos como esta cuestión que parece de resolución sencilla presenta graves problemas cuando la prestación laboral es desarrollada fuera de las instalaciones empresariales o dando lugar a la introducción de medios tecnológicos propiedad del trabajador, creando así una situación en la que el poder de dirección es más difuso y el control precisa del uso de medios distintos de los habituales, complicando de manera superior las garantías que la norma prevé respecto a la jornada y los descansos[90].

Por cuanto respecta a la jurisprudencia, apenas existen referencias al tema que ahora nos ocupa. Ya sea directamente en relación con un hipotético derecho a la desconexión digital o indirectamente en relación con otros posibles derechos en juego tales como, por ejemplo, la jornada (ordinaria o extraordinaria) de trabajo[91].

Tal es el caso del Tribunal Superior de Justicia de Castilla y León que en su sentencia 1523/2019[92] referente a un caso concerniente al agobio que los profesionales de justicia atravesaban ante las constantes notificaciones que recibían del sistema Lexnet aún fuera de horario laboral, expresó que "la imposición de una obligación de conexión digital […], puede entrar en contradicción con derechos fundamentales de los ciudadanos que se están reconociendo y configurando en el marco de la sociedad digital, como puede ser el derecho a la desconexión digital".

Ahora bien, ante el panorama que este derecho laboral digital llama a los convenios colectivos para una correcta e idónea ejecución del mismo, es el Convenio Colectivo del

[89] SERRANO GARCÍA, Juana Mª. La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia. cit. págs. 67 y ss.

[90] ORDOÑEZ PASCUA, Natalia. Relaciones de trabajo y ciberseguridad: nuevos retos en un futuro tecnológico incierto. cit. p. 264.

[91] BARRIOS BAUDOR, Guillermo L. El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones. cit. p. 13.

[92] STSJ CL 1523/2019, de 8 de abril.

Grupo AXA, de 21 de septiembre de 2017[93], quien fue pionero de incorporar a nivel interno de la empresa el derecho a la desconexión digital, previo a que el legislador considerara el mismo en la LOPDyGDD.

El Convenio Colectivo del Grupo AXA, bajo su Capítulo III sobre Organización del trabajo y nuevas tecnologías, estipula el art. 14 denominado "Derecho a la desconexión digital", en el que se apela directamente a los cambios tecnológicos que ya están en marcha y a las consecuencias que la interconectividad digital está produciendo en el mundo del trabajo[94].

En este contexto, sigue señalando el convenio que "el lugar de la prestación laboral y el tiempo de trabajo, como típicos elementos configuradores del marco en el que se desempeña la actividad laboral, están diluyéndose en favor de una realidad más compleja en la que impera la conectividad permanente afectando, sin duda, al ámbito personal y familiar de los trabajadores y trabajadoras. Es por ello que las partes firmantes de este Convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Consecuentemente, salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo".

Innegablemente se le aplaude a Grupo AXA por sentar un precedente ante la valoración de este derecho concerniente a los trabajadores, pero ¿qué significa "salvo fuerza mayor o circunstancias excepcionales"?

Primeramente, debemos remarcar que "salvo fuerza mayor o circunstancias excepcionales" son términos que en derecho se conocen como conceptos jurídicos indeterminados.

Por lo tanto, estas circunstancias, al no estar debidamente definidas en la empresa bajo términos que sean claros y acordes a un nivel de emergencia que sean precisamente considerados y tolerables como justos y necesarios, serían una condicionante más de una

[93] Convenio Colectivo Grupo Axa. Disponible en: https://boe.es/boe/dias/2017/10/10/pdfs/BOE-A-2017-11622.pdf

[94] GORDO GONZÁLEZ, Luis. El Derecho del Trabajo 2.0: la necesidad de actualizar el marco de las relaciones laborales a las nuevas tecnologías. cit. p. 182.

posible vulneración al derecho a la desconexión digital, debido a que realmente si no existe esa delimitación, para el empleador cualquier situación podría considerarse de emergencia, encaminando al trabajador a que independientemente del horario en el que se le realiza el llamado o cualquier otro tipo de comunicación, se vea obligado a atenderlos y llevar a cabo lo solicitado.

Es así que, sentamos precedente en decir que es a nivel de empresa mediante convenios colectivos, políticas, códigos de buenas prácticas, entre otros, en el que se deben de establecer los criterios necesarios para que tanto el empleador como el trabajador actuen de la manera correcta.

¿Y que pasa cuando entra en juego el BYOD?, ¿Cómo el trabajador ve expuesto su derecho a la desconexión digital?, ¿Cómo el empleador puede respetar y llevar a cabo un correcto control sobre ese aspecto?

Ante tales incógnitas, debemos reflexionar y concluir que el BYOD conllevaría para el trabajador una increíble dificultad para lograr una correcta separación entre su vida personal y familiar y su vida profesional, consiguiendo que de esta manera no se pueda conciliar la ejecución del derecho a la desconexión digital cuando este sea oportuno ejercerlo.

El empleador ante tal bifurcación deberá optar por las mejores medidas para impedir que se vulnere dicho derecho, ya que el trabajador al hacer uso de sus propios dispositivos móviles para uso laboral queda totalmente expuesto a recibir llamados, correos electrónicos, notificaciones y/o cualquier otro tipo de comunicación por parte de la empresa fuera de horario laboral.

Sin embargo, no solo el derecho debe buscar una solución ante tales problemáticas, sino que también la tecnología debe de ser una aliada a la hora de limitar las injerencias de lo laboral en horarios fuera de jornada, sacándole el mayor provecho a las mismas mediante por ejemplo sistemas y/o aplicativos instalados en los dispositivos de los trabajadores, con el objetivo de que se restrinja recibir cualquier tipo de notificación, llamada, mensaje o correo electrónico fuera de horario laboral.

Es indiscutible que el BYOD es una tendencia cada vez mas fuerte y por ello es necesario combinar las leyes que correspondan y las TICs para que se respeten los derechos de los trabajadores y las empresas también logren jornadas efectivas de trabajo, alcanzando así, una armonía juridico-laboral ante el respeto y ejecución de los derechos laborales digitales de los trabajadores.

4.2.4 Derecho a la propia imagen de los trabajadores

Ya no es novedad aludir a la importante transformación que se ha producido en el ámbito laboral como consecuencia de la introducción y el desarrollo de las TICs[95] y nuevas tendencias tecnológicas como el BYOD.

Sin embargo, como ya se ha advertido previamente, al contarse con una regulación no muy madura en estos temas en el fuero laboral, la irrupción de las TICs conlleva a la posible vulneración de derechos fundamentales como el derecho a la protección de la propia imagen de los trabajadores.

La CE alude en dos preceptos al derecho a la propia imagen. Por un lado y como hemos visto con anterioridad, en el art. 18.1 se produce su reconocimiento cuando se refiere a que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen" y, por otro, en el art. 20, apartado 4, donde se reiteran estos derechos como límites a la libertad de expresión e información[96].

No obstante, la norma laboral ni siquiera realiza un reconocimiento explícito al derecho a la propia imagen, aunque se hace una referencia a la dignidad de los trabajadores (art. 4.2 e) ET) que, como ya hemos venido insistiendo, es un valor jurídico fundamental al que se vinculan íntimamente los derechos reconocidos en el art. 18 CE. Esta ausencia normativa se extiende a la mayoría de los derechos cuyo contenido no es propiamente laboral y que en

[95] ARRÚE MENDIZÁBAL, Marta. *El derecho a la propia imagen de los trabajadores.* Pamplona: Aranzadi, 2019, pág. 325.

[96] ARRÚE MENDIZÁBAL, Marta. Op. cit. págs. 40 y ss.

afortunada terminología, se han denominado como derechos fundamentales inespecíficos del trabajador[97].

En la primera versión del ET, se optó por una norma que regulaba los aspectos esenciales de la relación de trabajo, perdiendo la oportunidad de establecer un sistema de garantías de los derechos de la persona trabajador. La única mención a estos derechos es lo previsto en algunos de los apartados del artículo 4, en el artículo 17 (que consagra la no discriminación en las relaciones laborales) y de manera tangencial, en los artículos 18 y 20 ET. En este último caso, más con una finalidad de respaldar o incluso ampliar las facultades empresariales, que de actuar como una barrera a las mismas en defensa de los derechos fundamentales de los trabajadores[98].

Con el uso de las nuevas tecnologías, de entre los diferentes sistemas de control que suelen emplearse en las empresas, los que parece que podrían afectar directamente al derecho a la propia imagen de los trabajadores son aquellos que permiten la grabación o captación de imágenes y que, en ocasiones, suelen ir también acompañados de la grabación del sonido. El creciente desarrollo tecnológico de estos instrumentos permite establecer un control mucho más amplio o extenso, en tiempo real y permanente[99], y que si no se respetan las garantías necesarias al respecto, desencadenaría un conjunto de problemas jurídicos muy graves.

No es así que hasta en el año 2018, el legislador sabiendo que existe una laguna normativa ante una correcta regulación de los aspectos de videovigilancia en la jornada de trabajo, decide como parte del conjunto de derechos laborales digitales recogidos en el Titulo X de la LOPDyGDD, establecer el art. 89 sobre derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, siendo este especifico en las facultades que habilitan al empleador para ejercer este tipo de control (art. 89.1[100]), como

[97] ARRÚE MENDIZÁBAL, Marta. Op. cit. págs. 40 y ss.

[98] ARRÚE MENDIZÁBAL, Marta. Op. cit. págs. 40 y ss.

[99] ARRÚE MENDIZÁBAL, Marta. Op. cit. págs. 323 y ss.

[100] Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Artículo 89.1. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo:* 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 […]. Los empleadores habrán

también los requisitos y limitantes del mismo ante su posible implantación en la empresa (art. 89.2 y art. 89.3).

Si bien es cierto que la videovigilancia expresada en el art. 89 es pensada y delimitada respecto a la instalación de cámaras de video y sistemas de audio en las instalaciones físicas de la empresa, el artículo pone de manifiesto que de no existir un deber de información por parte del empleador ante el uso de dichas medidas de control y vigilancia y una debida proporcionalidad del mismo, no estaríamos solamente vulnerando el derecho a la intimidad, sino también a la propia imagen del trabajador. Debemos tener en cuenta también que el conjunto de imágenes o sonidos captados con estas herramientas da paso a un tratamiento de datos de carácter personal.

Lo referenciado entonces respecto al análisis del art. 89, es de gran importancia si queremos trasladar lo allí previsto al BYOD, toda vez que, al ser los dispositivos propios del trabajador, las medidas de vigilancia en cuestión lograrían una injerencia aun mayor en los derechos fundamentales en juego, siendo un desafío como se pacte y regule la protección de los mismos ante las nuevas tendencias tecnológicas.

Como referencia jurisprudencial, el TEDH en su sentencia de 9 de enero de 2018, Asunto López Ribalda y Otros v. España[101], se manifiesta contra la opinión de los tribunales españoles respecto de la concurrencia de la proporcionalidad y expone que "El Tribunal observa que la videovigilancia llevada a cabo por el empleador […] no cumplió con […] la obligación de explícitar previamente informe de manera precisa e inequívoca a los interesados sobre la existencia y las características particulares de un sistema que recopila datos personales. El Tribunal observa que los derechos del empleador podrían haberse salvaguardado, al menos en cierta medida, por otros medios, en particular informando previamente a los solicitantes, incluso de forma general, sobre la instalación de un sistema de videovigilancia y proporcionándoles la información prescrita en la Ley de Protección de Datos Personales".

---

de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

[101] TEDH, Sentencia 9 de enero de 2018.

Será muy difícil trasladar este escenario jurídico al BYOD, porque se generan muchos conflictos, dado a que primeramente tal como en el caso anterior se produce una clara violación al derecho a la intimidad, ya que más allá de que el empleador informe a los trabajadores sobre estas medidas de control, se está accediendo a características particulares del dispositivo móvil como ser la cámara y el micrófono, siendo este último desde un punto de vista objetivo, un acceso desmesurado e innecesario, salvo esos tipos de trabajos en los que si se requiera ese control, por ejemplo un trabajo de operario en un Call Center.

Por lo tanto, ante tales escenarios entraría en este ámbito los principios de proporcionalidad e intervención mínima que nos expresa el art. 89.3, ya que de no hacerlo, estaríamos frente a una intromisión excesiva a la vida personal del trabajador, además ¿cómo asegura el trabajador que esos sistemas de videovigilancia no serán ejecutados fuera de la jornada laboral?

Recordemos que el trabajador al usar sus propios dispositivos móviles, estos no son solo usados meramente para fines estrictamente profesionales, sino también personales, es así que su imagen e intimidad como tal se ven expuestas al ser captadas por este tipo de herramientas, sin dejar de lado que también podrían verse afectados los derechos de terceros.

Por consiguiente, sería recomendable que el empleador haga uso de mecanismos de control menos invasores y lesivos a derechos fundamentales y laborales digitales, como ser, aplicativos o sistemas para gestión del tiempo, organizadores de tareas, cumplimiento de actividades, entre otros; ya que no es necesario monitorear una cámara para poder apreciar si el trabajador está ejerciendo labores en tiempo y forma, sino que también con indicadores de cumplimiento al día a día se podrá saber que tan productivo es el mismo.

Con todo lo anterior, es evidente la existencia de una brecha normativa que debe esclarecerse lo más rápido y oportuno posible en el ordenamiento jurídico español. Tal como se evidenció en este apartado, no es suficiente la regulación que se cuenta para proteger el derecho en cuestión.

No podemos asemejar una videovigilancia en una empresa, fábrica o sector físico, al acceso y control de la cámara y audio del trabajador en su propio dispositivo. Más que nunca la

finalidad y proporcionalidad deben ser los principios que rigan las decisiones del empleador a la hora de aplicar herramientas tecnológicas en dispositivos que pertenecen al trabajador y que conllevan a una intromisión excesiva en los mismos, tornando como consecuencia una peligrosa vulneración de derechos fundamentales y laborales digitales.

4.3 Regulación convencional y guías de buenas prácticas

Dado al elevado desarrollo e implantación de las nuevas tecnologías en ámbito laboral, los acuerdos o negociación colectiva tienen un papel destacado en las relaciones laborales para llevar a cabo una regulación jurídica de las TICs en la empresa[102].

La OIT define a la negociación colectiva como "un mecanismo fundamental del diálogo social, a través del cual los empleadores y sus organizaciones y los sindicatos pueden convenir salarios justos y condiciones de trabajo adecuadas; además, constituye la base del mantenimiento de buenas relaciones laborales"[103].

Con respecto al ordenamiento jurídico español, conviene destacar que el ET recoge en su Título III "De la negociación colectiva y de los convenios colectivos", todas las disposiciones generales de los mismos (eficacia, concurrencia, contenido, vigencia, entre otros), como también el procedimiento a seguir para ejecutar bajo lo expresamente señalado por el ET, esta vía de conciliación empresarial.

Es así como en los últimos años se ha venido reflejando que, los empleadores en conjunto con los representantes de los trabajadores han mejorado muchas situaciones entorno a diferentes condiciones laborales, como ser la jornada del trabajo, horario y distribución del tiempo de trabajo, trabajo por turnos, sistemas de remuneración, funciones del trabajador, entre otros. Constatando así que los convenios colectivos han sido un aliado al momento de regular esos factores y muchos más.

---

[102] SERRANO GARCÍA, Juana Mª. La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia. cit. p. 17.

[103] ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *Negociación colectiva y relaciones laborales*. [en línea]. Disponible en: https://www.ilo.org/global/topics/collective-bargaining-labour-relations/lang--es/index.htm

En materia de derechos laborales digitales, el art. 91 de la LOPDyGDD es donde el legislador remarca la importancia de los convenios colectivos, expresando que "los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

Lo anterior deja abierta a la negociación colectiva la posibilidad de establecer y concretar medidas adicionales que, para determinados sectores empresariales o según la idiosincrasia de determinadas empresas, seguramente, serán necesarias para garantizar una protección de los derechos digitales concernientes a los trabajadores[104].

Ante lo expuesto, es notorio expresar que el alcance de la negociación colectiva del art. 91 es bastante limitado y como hemos visto en apartados anteriores, parece que la figura estrella es el derecho a la desconexión digital, porque ha sido el medio que determina la pauta justa y necesaria para hacer valer dicho derecho[105].

Aun así, es de esperar que en los futuros convenios colectivos se recojan más derechos y así los mismos tengan una mayor concreción para el cumplimiento de sus garantías.

En relación al BYOD, los convenios colectivos tendrán un papel protagonista, ya que con ellos serán muchas las empresas que exitosamente puedan llegar a pautar que una vez dada la incursión de los dispositivos móviles propiedad del trabajador en la empresa, cual será el uso permitido que este debe de hacer de los mismos durante la jornada de trabajo.

De igual manera, el desarrollo e implementación de guías de buenas prácticas sobre el uso de las nuevas tecnologías, será también una buena vía para conciliar un ambiente de trabajo propicio ante entornos BYOD, pero estas deben promoverse adecuadamente y formar parte integral de las políticas de la empresa.

---

[104] BIURRUN ABAD, Fernando. *Negociación colectiva de los derechos digitales*. [en línea]. Disponible en: https://www.legaltoday.com/legaltech/nuevas-tecnologias/negociacion-colectiva-de-los-derechos-digitales-2019-01-31/

[105] BIURRUN ABAD, Fernando. Op. cit.

Es importante destacar que estas guías de buenas prácticas deberán estar dirigidas a todos los trabajadores de la empresa. En ellas se definirán detalladamente y con base a una serie de necesidades existentes y previamente detectadas por el empleador, un conjunto de conductas y directrices que ayuden a satisfacer la correcta incorporación y uso de las nuevas tecnologías o tendencias tecnológicas como el BYOD a la empresa.

De esta forma, con el desarrollo de las mismas, se fomentará positivamente que el empleador es un promotor del uso de las TICs como medio aliado de los trabajadores para el desarrollo de sus labores diarias, siempre y cuando los mismos hagan un uso consciente y no desmesurado de ellas, más cuando estas tecnologías son propiedad de ellos mismos (claro esta, durante la jornada laboral).

Aunque el BYOD es una tendencia que apunte a ir en crecimiento con el paso de los años, y pese a que el derecho se mantiene por detrás de eso, representando una carrera inalcanzable en el que siempre termina en segundo lugar, existen otros medios como los anteriormente expuestos para regular y definir sistemáticamente una acertada conciliación entre el BYOD y su impacto con los derechos fundamentales y laborales digitales.

V. RECOMENDACIONES PARA UNA CORRECTA IMPLEMENTACIÓN DEL BYOD.

Si hasta ahora los empleadores tenían que lidiar con el uso privado que los trabajadores hacen con los dispositivos tecnológicos propiedad de la empresa, ahora tienen que hacer frente a los dispositivos móviles propiedad del trabajador, que son mucho más potentes y versátiles que los que la empresa pone a su disposición[106], pero ¿cuál será el mejor camino a seguir para actuar ante dicho escenario?

Sin duda alguna, no hay un método específico que el empleador deba seguir, todo dependerá del caso en concreto de cada una de las empresas, pero este en definitiva deberá actuar de manera proactiva y muchas veces reactiva para atacar positivamente esta tendencia, estableciendo una serie de instrumentos, herramientas tecnológicas y/o mecanismos oportunos para una correcta implementación del BYOD en la empresa.

Es así que en este apartado, brindaremos de manera muy puntual una serie de recomendaciones que aplicadas adecuadamente en la empresa ofrecerán una visión clara y estratégica para hacer frente a los riesgos del BYOD.

5.1 Política de Seguridad y Uso del BYOD

Independientemente de la posición que adopte la empresa con respecto a la implementación del BYOD, es necesario que la misma actúe diligentemente en pro de garantizar la seguridad de la información frente al uso de los dispositivos móviles[107].

Es así como el Departamento de Tecnologías de la Información (en adelante, Departamento de TI) junto con la gerencia de la empresa, deberá inicialmente evaluar los posibles riesgos que generen un impacto ante el uso de estos dispositivos, que hoy en día son parte de los medios utilizados por el trabajador durante la jornada de trabajo.

---

[106] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 121.

[107] ESET LATINOAMÉRICA. *Retos de seguridad para las empresas a partir de BYOD* [en línea]. 2012, pág. 3. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/seguridad_en_byod.pdf

Una vez identificado estos riesgos y con el fin de minimizar la materialización de cualquier amenaza, el Departamento de TI deberá definir una política de seguridad y uso del BYOD, con el principal objetivo de generar en la empresa las normas de usabilidad, acciones proactivas y reactivas en materia de seguridad informática, prácticas formativas y de concientización a los trabajadores en el manejo de los dispositivos móviles en un entorno BYOD[108].

Asimismo, una de las medidas más importantes que deberán adoptar las empresas será la de incluir en esa política, los requisitos técnicos y de seguridad que deberán cumplir los dispositivos móviles propiedad del trabajador para que estos sean habilitados a poder alojar aplicaciones y datos pertenecientes a la empresa[109].

Estos requisitos técnicos y de seguridad pueden cubrir la exigencia de contar con sistemas operativos de los dispositivos móviles actualizados al día, parches de seguridad debidamente aplicados, antivirus instalados (en caso que se requiera), contraseñas robustas y cambios de las mismas periódicamente para acceder a los recursos de la empresa, uso de VPN[110] (*Virtual Private Network* por sus siglas en ingles, *Red Privada Virtual* en castellano) para conexiones más seguras y cifradas al acceder a servicios críticos de la empresa, restringir el uso de aplicaciones de terceros instaladas en los dispositivos, entre otros.

El CCN evidencia que "pese a la importancia capital de contar con una Política de Seguridad BYOD, diversos estudios señalan que aproximadamente el 60 por ciento de las organizaciones reconoce que no tienen una política especifica sobre cómo los empleados pueden usar sus propios dispositivos en el lugar de trabajo y, lo que es más preocupante, uno

---

[108] GOVERTIS ADVISORY SERVICES. *Políticas BYOD Y MDM* [en línea]. Disponible en: https://dpd.aec.es/politicas-byod-y-mdm/

[109] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 122.

[110] Una VPN es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet como el medio para llevarlo a cabo. Hoy más que nunca, las empresas suelen utilizar estas redes para que sus trabajadores, desde sus casas, hoteles, etcétera, puedan acceder a recursos corporativos que, de otro modo, no podrían. GOUJON, André. *¿Qué es un VPN y cómo funciona para la privacidad de la información?* [en línea]. Disponible en: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

de cada cuatro reconoce que hacen excepciones para el personal directivo, precisamente aquel que puede acceder y almacenar la información más relevante para la organización y que suele ser el principal objetivo de los ciberataques dirigidos (ciberespionaje político o industrial)"[111].

Es así que, en pocas palabras la política de seguridad y uso del BYOD deberá delimitar qué cosas puede hacer un trabajador y cuales no con el uso de sus propios dispositivos en la empresa y en qué medida poder hacerlo. Además, esta política deberá ser de estricto cumplimiento para todos los miembros pertenecientes a la empresa, sin excepción alguna, aunque su alcance y aplicación varíe para los trabajadores en función de su puesto de trabajo.

También, una vez creada la política de seguridad y uso del BYOD, esta debe ser divulgada a todo el personal, para que todos los niveles de la organización (incluidos los altos directivos) conozcan las restricciones de sus dispositivos y de acceso a los diferentes recursos pertenecientes a la empresa[112].

Además, previa aplicación de dicha política, se considerará necesaria la firma de un documento de conformidad y aceptación de la misma por parte del trabajador, antes de su utilización en la empresa[113]. Lo anterior porque son los dispositivos de ellos por los que la política tiene sentido de ser.

Un buen plan de divulgación será la clave para que la empresa promueva de la mejor manera posible la política y así el trabajador tenga un sentido de cumplimiento y pertenencia con la misma.

Por lo tanto, una exitosa implementación del BYOD combina la sencillez para los trabajadores y los empleados, además de una seguridad, un control y una administración

[111] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. p. 19.

[112] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Op. cit. p. 24.

[113] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario. cit. p. 19.

efectiva para el Departamento de TI. Y aunque éste puede verse tentado de desarrollar políticas específicas para todas y cada una de las situaciones posibles, lo cierto es que la mayoría de las consideraciones se pueden contemplar aplicando unos cuantos principios sencillos y coherentes[114], por ejemplo, el uso de correo electrónico en los celulares solo será exclusivamente para gerentes de área y los trabajadores que bajo indicaciones de ellos deban tener el mismo acceso.

5.2 Soluciones MDM (Mobile Device Management)

Gozar de una infraestructura de TI lo suficientemente robusta a nivel de hardware y software para hacer frente a la implementación del BYOD, será el factor de diferenciación que las empresas deberán considerar para lograr un ambiente tecnológico-empresarial propicio al uso de dispositivos móviles durante las jornadas de trabajo.

Es así que una vez aprobado el uso del BYOD, las empresas pueden adquirir y hacer uso de diferentes soluciones tecnológicas, que integradas en su infraestructura de TI, les permitan ejecutar una adecuada y oportuna gestión de los dispositivos móviles a nivel empresarial.

Una de estas soluciones se conoce como MDM (*Mobile Device Management* por sus siglas en inglés, *Gestión de Dispositivos Móviles* en castellano). Este tipo de soluciones permiten gestionar de forma eficiente la diversidad y el despliegue masivo, dinámico y a gran escala de los dispositivos móviles en la empresa (sean estos propiedad de los trabajadores o no), con un enfoque principalmente orientado a incrementar la seguridad informática, así mejorando colateralmente la productividad del usuario final, en este caso, el trabajador[115] y pudiendo ser aplicadas a los principales sistemas operativos utilizados en la actualidad: Android de Google, iOS de Apple, Windows Phone de Microsoft[116], entre otros.

---

[114] PUYOL, Javier. Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa. cit. p. 51.

[115] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. págs. 21 y ss.

[116] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). *Guía de Seguridad de las TIC (CCN-STIC-457) Gestión de dispositivos móviles: MDM (Mobile Device*

Este tipo de soluciones multiplataforma, es decir, con la que se pueden gestionar diferentes tipos de sistemas operativos y marcas, facilitará al empleador poder administrar el uso de dispositivos móviles propiedad de los trabajadores como instrumentos de acceso a recursos que son propiedad de la empresa[117].

Con la integración de una solución MDM adecuada y que esta satisfaga las necesidades que la empresa desea suplir, se tendrá incluso la capacidad de gestionar las aplicaciones móviles instaladas en los dispositivos, reduciendo así una brecha de seguridad muy alta ante algún posible ciberataque que afecte no solo al dispositivo como tal, sino también a la infraestructura de TI de la empresa. Recordemos que estos dispositivos al ser propiedad de los trabajadores pueden llegar a tener un número considerable de aplicaciones instaladas de fuentes no confiables y la empresa no se puede permitir que dado a eso se genere una violación a la confidencialidad, integridad y disponibilidad de sus activos de información.

Adicionalmente, con respecto a la gestión que se hará de los dispositivos móviles y de las aplicaciones instaladas en ellos, la industria ha identificado la necesidad de proteger los datos y contenidos corporativos distribuidos hacia o accedidos desde los dispositivos móviles, con arquitecturas y soluciones denominadas MCM (*Mobile Content Management* por sus siglas en ingles, *Gestión de Contenido Móvil* en castellano). Estas características MCM pueden llegar a estar disponibles dentro de la propia solución MDM, como una funcionalidad más[118].

Con las soluciones MDM, no hay intromisión a los dispositivos móviles de los trabajadores, una de sus principales características es la de configurar diferentes perfiles de seguridad y/o políticas que en su conjunto ayuden a alcanzar el enfoque que detallamos anteriormente, por ejemplo, puede establecerse una política de acceso delimitando que durante la jornada de trabajo no se pueda hacer uso de aplicaciones de streaming como ser las utilizadas para ver

---

Management) [en línea]. 2013, pág. 9. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-de-dispositivos-moviles-mdm/file.html

[117] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD). cit. p. 22.

[118] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). Guía de Seguridad de las TIC (CCN-STIC-457) Gestión de dispositivos móviles: MDM (Mobile Device Management). cit. págs. 9 y ss.

videos o escuchar música, pero las mismas si son permitidas durante el tiempo de descanso que posee el trabajador.

De esta manera podemos apreciar que se podrá conciliar de la mejor manera posible el uso de los dispositivos con restricciones apropiadas en tiempo y forma, pero sin llegar a afectar derechos fundamentales y/o laborales digitales de los trabajadores.

También es importante delimitar que, tanto estos permisos como restricciones habilitados a través de la solución MDM, deberán tener estrecha relación y concordancia con lo establecido en la política de seguridad y uso del BYOD, ya que en caso contrario, esto sí podría desencadenar situaciones ambiguas que pueden poner en riesgo la transparencia de lo que pueda o no hacer el trabajador, trayendo consigo algunos conflictos en materia jurídica.

Por lo expuesto anteriormente, concluimos que la solución MDM que se adquiera, deberá focalizar sus capacidades de gestión empresarial en tres ámbitos principales: dispositivos móviles, aplicaciones móviles y contenidos propiedad de la empresa (accedidos desde los dispositivos y/o aplicaciones móviles)[119].

Con esto garantizaremos no solo una gestión adecuada del BYOD, sino también la tranquilidad de saber que los trabajadores cuando hacen uso de sus propios dispositivos, lo están haciendo bajo unas directrices y métricas que la empresa previamente ha definido como las necesarias ante este tipo de circunstancias.

5.3 Implementación/configuración de otras herramientas tecnológicas

Las soluciones MDM no son el único aliado a considerar para una adecuada gestión de los dispositivos móviles. Si se contempla el panorama de todos los elementos tecnológicos que componen la infraestructura de TI de la empresa y si se saca el mayor provecho de los mismos, se puede llegar a armonizar mucho más el uso de estos dispositivos.

[119] CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT) Op. cit. p. 10.

Si hablamos de seguridad perimetral, el Firewall o cortafuegos, es la herramienta por excelencia que suple las necesidades de la empresa con respecto a monitorear el tráfico de red entrante y saliente[120] en función de un conjunto de parámetros ya previamente configurados en él.

El Firewall al ser una equipo potente, tendrá la capacidad de administrar este tráfico en función de la aplicación de varios tipos de filtros[121], como el horario en el que se debe ejecutar dichas políticas, los usuarios a los que van destinadas, los servicios, páginas web o aplicativos a los que se restringe o concede acceso, entre otras más. Como las políticas son totalmente personalizables, será cuestión del empleador como quiere ajustarlas.

Por consiguiente, si buscamos permitir o restringir el uso de ciertas aplicaciones o páginas web en específico, tan solo con definir algunas políticas de seguridad en el Firewall, estaremos acotando cada vez más el uso que se hará de los dispositivos móviles durante la jornada de trabajo.

Sin embargo, es importante apuntar que si el empleador desea una administración más minuciosa sobre estos dispositivos que conforman el entorno BYOD de la empresa, es el MDM la solución más propicia para llevarla a cabo, ya que el Firewall aunque nos ayude a mitigarlo, sus principales funcionalidades son otras, como detectar amenazas en la red.

A nivel de seguridad en redes inalámbricas, si la empresa cuenta con el despliegue de una red Wi-Fi, ésta deberá de proteger todo tipo de comunicación que se lleve a cabo mediante el uso de cualquier tipo de dispositivos conectados a esa red. Esto debido a que la red Wi-Fi

[120] Entenderemos por tráfico de red entrante y saliente a toda comunicación (enviar o recibir datos/información) entre usuarios, equipos y/o servicios conectados a la red informática institucional de la empresa, como también fuera de esta mediante el uso de internet. Una de las funcionalidades del Firewall es la de registrar cada envío o recibo de información que provenga dentro o fuera de la red informática de la empresa.

[121] Estos filtros son pensados para suplir las diferentes necesidades que el empleador quiere satisfacer en consecuencia de reducir los riesgos inherentes a la incursión en la empresa de dispositivos móviles personales propiedad del trabajador. Con estos filtros, se personaliza la acción que el Firewall ejecutará una vez sea habilitada la política en el mismo, siendo así una forma más especifica y controlada de administrar el uso de dichos dispositivos durante la jornada de trabajo.

es un foco principal y muy común para los ciber atacantes por los diferentes riesgos que estas acarrean si no se configuran y administran de la mejor manera[122].

El INCIBE indica que "para llevar a cabo una correcta configuración de seguridad en redes inalámbricas en el ámbito empresarial, será necesario distinguir entre los equipos que serán considerados como corporativos y equipos de personal externo"[123], en nuestro caso, estos equipos externos serán los dispositivos móviles de los trabajadores.

"Además, dentro de las políticas de seguridad con las que debe contar cualquier organización, deberá existir una específica donde queden reflejadas las medidas de protección y seguridad con las que deberá contar la red inalámbrica, estableciendo qué requisitos deberán cumplir, tanto los equipos corporativos (actualización de antivirus, parches del sistema operativo, política de actualizaciones de software, cortafuegos, etc.), como los dispositivos externos, que quieran conectarse a la misma"[124].

Por lo tanto, si la red Wi-Fi es muy demandada por los trabajadores y estos usan sus dispositivos móviles personales para conectarse a ella, no bastará por parte de la empresa contar con los equipos mínimos (por ejemplo, los AP[125]) para brindar este tipo de conexiones, sino que, se deberá considerar la implementación de equipos más robustos que ayuden a centralizar y administrar todo lo referente a la red Wi-Fi (como ser los equipos WLC[126]),

---

[122] Sin embargo, y como vimos en apartados anteriores, la exposición a estos riesgos, están más presentes al hacer uso de redes Wi-Fi públicas, que en una red Wi-Fi empresarial, que en teoría, es un entorno privado y controlado a la no intromisión de terceros. Es asi, que uno de los principales problemas con la incorporación del BYOD en la empresa con relación al uso de redes inalámbricas, es que los dispositivos móviles de los trabajadores que además de acceder a recursos de la empresa, también están almacenando información de la misma, en muchas ocaciones están (una vez terminada la jornada de trabajo) conectados a redes Wi-Fi públicas, siendo estos dispositivos un blanco perfecto para que los ciberatacantes obtengan información sensible, roben credenciales de acceso, etcétera.

[123] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Seguridad en redes wifi: una guía de aproximación para el empresario* [en línea], pág. 12. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

[124] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Op. cit. p. 12.

[125] Los AP (*Access Point*, por sus siglas en ingles o *Puntos de Acceso* en castellano), son los equipos utilizados y configurados para proveer y establecer una conexión inalámbrica que forma parte de la Red Wi-Fi de la empresa. Como parte de sus funcionalidades, con ellos se puede administrar diferentes características, como ser el nombre de la red, la contraseña de acceso, los dispositivos permitidos, entre otros.

[126] Si la empresa cuenta con muchos APs, es recomendable y altamente necesario centralizar toda la administración de los mismos en un solo equipo. Los WLC (*Wireless Lan Controller*, por sus siglas en ingles y *Controlador Lan Inalámbrico* en castellano) es el dispositivo utilizado para dicha cuestión. Si se desea

como también definir directrices claras y específicas en la materia, que estén debidamente estipuladas en la Política de Seguridad de la empresa.

De igual manera y como lo hemos contemplado en apartados anteriores, una ventaja indiscutible del BYOD es la movilidad que brinda a los trabajadores al poder trabajar en cualquier lugar, pero si necesitamos acceder a recursos de la empresa mediante una red pública, deberemos crear canales seguros cifrados de comunicación. Es por eso que recurrir al uso de VPN es la mejor opción. De esta forma nos podemos conectar de forma segura a través de esas redes (cuya seguridad desconocemos), garantizando así, la confidencialidad e integridad de la información que transmitimos[127].

Asimismo, en el mercado existen diferentes soluciones que complementadas con los dispositivos detallados anteriormente, preservan mucho más la seguridad de la información de la empresa, haciendo frente al uso de dispositivos móviles en un entorno BYOD. Tal es el caso de los DLP (*Data Loss Prevention*, por sus siglas en inglés y *Prevención de Pérdida de Datos* en castellano)[128].

Una vez implementadas estas herramientas, su función es monitorear el uso de la información, encargándose de hacer cumplir las políticas relacionadas con el manejo de los datos clasificados como confidenciales. De esta forma, una solución DLP bloquea intentos de filtración no autorizados, al mismo tiempo que permite el uso apropiado de los datos[129].

---

cambiar una configuración de la red inalámbrica de la empresa, no será necesario ir AP por AP cambiando los parámetros, sino que con ejecutar el cambio en el WLC, este se replicará absolutamente a todos los AP, facilitando así la administración de la red Wi-Fi de la empresa.

[127] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario. cit. p. 17.

[128] DLP hace referencia a todas las estrategias pensadas para mantener los datos sensibles dentro de la red informática de la empresa, protegiéndolos de filtraciones accidentales o maliciosas, de manera que solo sean compartidas con quién y como el empleador decida. También es el nombre que recibe el conjunto de herramientas tecnológicas diseñadas para facilitar esta labor. CHISTIK, Javier. *¿Qué es Data Loss Prevention?* [en línea]. Disponible en: https://www.forcepoint.com/es/blog/insights/what-is-data-loss-prevention-dlp

[129] CHISTIK, Javier. Op. cit.

Con el uso del BYOD, las filtraciones de información están a la orden del día, por lo que contar con este tipo de soluciones que se ajustan a reducir esta brecha de seguridad, es una gran vía de prevención.

Ante todo lo expuesto, debemos tener claro que el hecho de que los dispositivos móviles personales de los trabajadores puedan acceder y manejar información confidencial y sensible para las empresas, esto debe hacer pensar al empleador a tomar precauciones especiales a la hora de trabajar con ellos[130].

Tanto los propios dispositivos como la información que se maneja deben estar protegidos convenientemente, estableciendo unas buenas políticas y configuraciones de seguridad[131] con las que se logre edificar el ambiente empresarial ideal en el que el BYOD no sea considerado un factor de vulneración a derechos fundamentales o laborales digitales de los trabajadores, ni mucho menos, un enemigo para la seguridad de la información de la empresa, sino como un aliado para el desarrollo de las funciones laborales, como también un elemento tecnológico presente, que aunque transporta mucho riesgos en materia de seguridad informática, puede ser administrado y controlado de la mejor manera posible si el empleador actúa en consecuencia una vez identificado el auge de esta tendencia tecnológica en la empresa.

[130] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Cinco consejos para la utilización segura de BYOD* [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/cinco-consejos-utilizacion-segura-byod

[131] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Op. cit.

CONCLUSIONES

A la luz de las reflexiones anteriores, cabe extraer las siguientes conclusiones:

PRIMERA. *Las TICs son un componente esencial para el desarrollo de las relaciones laborales en la era digital.* La transformación digital que han estado afrontando las empresas a lo largo de los últimos años ha sido el elemento indispensable para entender y comprender que la digitalización conlleva un conjunto de herramientas que puestas a disposición del empleador y el trabajador, y empleadas responsablemente por ellos, pueden ser consideradas como un aliado justo y necesario para el desarrollo de la actividad laboral de la empresa, que ayuda a mejorar la productividad y la competitividad.

SEGUNDA. *El BYOD, que consiste en la aportación por el trabajador de los instrumentos digitales de trabajo, es una tendencia tecnológica que llegó a las empresas para quedarse.* Las estadísticas y la situación actual en la que las empresas se ven inmersas por el auge de las nuevas tecnologías, nos indican que el BYOD es una tendencia que con el paso de los años irá creciendo exponencialmente y por consiguiente, serán muchos los empleadores y trabajadores que irán disponiendo de ella y adaptándola a su quehacer productivo.

TERCERA. *Los riesgos jurídico-laborales por el impacto del BYOD son inminentes.* Es así, que de no contar el empleador con la diligencia necesaria para hacer frente a esta tendencia en auge en este utillaje, puede provocar a que el trabajador se vea envuelto en una posible vulneración de algunos de sus derechos fundamentales y laborales digitales, ya que el uso de sus propios dispositivos móviles para fines profesionales abren el camino para generar diferentes problemas que hasta el día de hoy el derecho no tiene contemplados.

CUARTA. *La legislación laboral actual no se detiene en abordar el BYOD y los riesgos derivados de este.* Es apremiante hacer notar que los avances de la tecnología y todo lo que esto conlleva van un paso por delante de una posible regulación de las mimas en materia legislativa. Debido a estas carencias, hemos podido apreciar como existe una serie de lagunas normativas para regular el impacto jurídico-laboral que acarrea el uso de los dispositivos móviles personales del trabajador en la jornada de trabajo. Para esto, el legislador deberá considerar adaptar algunos de los preceptos normativos expuestos en este trabajo para así

regular el BYOD en tiempo y forma, principalmente por lo que se refiere a dos extremos capitales: por un lado, la supervisión del uso que realizan los trabajadores sobre tales dispositivos al objeto de garantizar un rendimiento laboral óptimo; por otro, los problemas de seguridad ante la posible fuga de información empresarial.

QUINTA. *El poder de control del empresario no faculta en su totalidad para extralimitarse hacia los dispositivos móviles personales del trabajador.* Si el dispositivo no es propiedad de la empresa, aunque exista un interés legítimo por parte del empleador para llevar a cabo un control de tal herramienta, este debe ser estrictamente proporcional y no extralimitado, guardando el debido respeto a los derechos fundamentales del asalariado.

SEXTA. *Los convenios colectivos, las guías de buenas prácticas y demás protocolos internos de la empresa, son los medios más adecuados e imprescindibles para hacer frente a una posible regulación del BYOD.* Si bien es cierto, cada empresa abordará de manera diferente el BYOD, hasta el día de hoy son los convenios colectivos, las guías de buenas prácticas y demás documentos normativos y/o disciplinarios internos de la empresa, como pueden ser las políticas de seguridad, los cauces más certeros para regular desde un punto de vista jurídico y técnico el BYOD. De esta manera, es fundamental otorgarle importancia y más relieve a estos instrumentos, ya que con ellos se puede lograr conciliar la salvaguarda de los derechos laborales digitales de los trabajadores, así como también evitar los problemas de seguridad de la información.

BIBLIOGRAFÍA

- ARRÚE MENDIZÁBAL, Marta. *El derecho a la propia imagen de los trabajadores.* Pamplona: Aranzadi, 2019.

- BARRIOS BAUDOR, Guillermo L. "El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones". *Revista Aranzadi Doctrinal* [en línea]. 2019, núm. 1, pp. 1-21. Disponible en: dialnet.unirioja.es/servlet/articulo?codigo=6771678

- BAZ RODRIGUEZ, Jesús. *Privacidad y protección de datos de los trabajadores en el entorno digital.* Madrid: Wolters Kluwer, 2019.

- BIURRUN ABAD, Fernando. *Negociación colectiva de los derechos digitales*. [en línea]. Disponible en: https://www.legaltoday.com/legaltech/nuevas-tecnologias/negociacion-colectiva-de-los-derechos-digitales-2019-01-31/

- BRADLEY, Joseph; LOUCKS, Jeff; MACAULAY, James; MEDCALF, Richard y BUCKALEW, Lauren. *BYOD: una perspectiva global. Estudio Horizons Cisco IBSG acerca de las tendencias BYOD y de virtualización* [en línea]. 2012, pp. 1-21. Disponible en: https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons-Global_ES.pdf

- BULLOCK, Lilach. *The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future* [en línea]. Disponible en: https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/

- CALLE, Vicente. *BYOD, "utiliza tu dispositivo personal para trabajar", la nueva revolución* [en línea]. Disponible en: https://www.garrigues.com/es_ES/noticia/byod-utiliza-tu-dispositivo-personal-para-trabajar-la-nueva-revolucion

- CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). *Informe de amenazas CCN-CERT IA-21/13: riesgos y amenazas del Bring Your Own Device (BYOD)* [en línea]. 2013, pp. 1-27. Disponible

en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html

- CAPACIDAD DE RESPUESTA A INCIDENTES DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT). *Guía de Seguridad de las TIC (CCN-STIC-457) Gestión de dispositivos móviles: MDM (Mobile Device Management)* [en línea]. 2013, pp. 1-97. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-de-dispositivos-moviles-mdm/file.html

- CHISTIK, Javier. *¿Qué es Data Loss Prevention?* [en línea]. Disponible en: https://www.forcepoint.com/es/blog/insights/what-is-data-loss-prevention-dlp

- CREMADES CHUECA, Oriol. "Impacto teórico-práctico del BYOD en el derecho del trabajo". *Revista de Trabajo y Seguridad Social* [en línea]. 2018, núm 2018, pp. 103-122. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6470608

- CRUZ VILLALÓN, Jesús. "Las transformaciones de las relaciones laborales ante la digitalización de la economía". *Temas Laborales: Revista andaluza de trabajo y bienestar social* [en línea]. 2017, núm. 138, pp. 13-47. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6552388

- DEL REY GUANTER, Salvador. "Relaciones laborales y nuevas tecnologías: reflexiones introductorias", en AA.VV. (DEL REY GUANTER, Salvador, Dir. y LUQUE PARRA, Manuel, Coord.): *Relaciones Laborales y Nuevas Tecnologías* [en línea]. Madrid: La Ley, 2005, pp. 1-8. Disponible en: https://books.google.es/books?id=osR5WCpKxX8C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- DÍAZ REVORIO, F. Javier. "El derecho fundamental al secreto de las comunicaciones". *Derecho PUCP: Revista de la Facultad de Derecho* [en línea]. 2006, núm. 59, pp. 159-175. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5085108

- ESET LATINOAMÉRICA. *Retos de seguridad para las empresas a partir de BYOD* [en línea]. 2012, pp. 1-12. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/seguridad_en_byod.pdf

- FERNÁNDEZ ORRICO, Fco. Javier. "Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre". *Revista Española de Derecho del Trabajo* [en línea]. 2019, núm. 222, pp. 31-76. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7059685

- GONZÁLEZ GONZÁLEZ, Carlos. "Control empresarial de la actividad laboral y uso de las nuevas tecnologías". *Revista Aranzadi Doctrinal* [en línea]. 2015, núm. 11, pp. 111-128. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5319216

- GORDO GONZÁLEZ, Luis. "El Derecho del Trabajo 2.0: la necesidad de actualizar el marco de las relaciones laborales a las nuevas tecnologías". *Revista de Información laboral* [en línea]. 2017, núm. 12, pp. 171-182. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6283319

- GOUJON, André. *¿Qué es un VPN y cómo funciona para la privacidad de la información?* [en línea]. Disponible en: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

- GOVERTIS ADVISORY SERVICES. *Políticas BYOD Y MDM* [en línea]. Disponible en: https://dpd.aec.es/politicas-byod-y-mdm/

- GRISOLIA, Julio Armando. *Manual de Derecho Laboral* [en línea]. Ciudad Autónoma de Buenos Aires, Argentina: Abeledo Perrot, 2019. Disponible en: https://proview-thomsonreuters-com.digitalbd.uade.edu.ar

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Bondades y riesgos del BYOD* [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/bondades-y-riesgos-del-byod

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Cinco consejos para la utilización segura de BYOD* [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/cinco-consejos-utilizacion-segura-byod

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario* [en línea]. 2017, pp. 1-22. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Seguridad en redes wifi: una guía de aproximación para el empresario* [en línea]. 2019, pp. 1-30. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

- KARANACUS, Chris. *Half of Companies Will Require BYOD By 2017, Gartner Says* [en línea]. Disponible en: https://www.cio.com/article/2386248/half-of-companies-will-require-byod-by-2017--gartner-says.html

- NARANJO COLORADO, Luz Dary. "Vicisitudes del nuevo derecho a la desconexión digital: Un análisis desde la base del derecho laboral". *Revista Saber, Ciencia y Libertad* [en línea]. 2017, núm. 2, pp. 49-57. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6556861

- ORDOÑEZ PASCUA, Natalia. "Relaciones de trabajo y ciberseguridad: nuevos retos en un futuro tecnológico incierto". *Revista General de Derecho del Trabajo y de la Seguridad Social* [en línea]. 2019, núm. 53, pp. 246-279. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7013608

- ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *La Relación de Trabajo* [en línea]. 2006, pp. 1-95. Disponible en: http://www.ilo.org/public/spanish/standards/relm/ilc/ilc95/pdf/rep-v-1.pdf

- ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *Negociación colectiva y relaciones laborales*. [en línea]. Disponible en: https://www.ilo.org/global/topics/collective-bargaining-labour-relations/lang--es/index.htm

- PANETTA, Kasey. *Gartner Top Strategic Predictions for 2020 and Beyond* [en línea]. Disponible en: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2020-and-beyond/

- PÉREZ CAMPOS, Ana Isabel. "La desconexión digital en España: ¿un nuevo derecho laboral?". *Anuario Jurídico y Económico Escurialense* [en línea]. 2019, núm. 52, pp. 101-124. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6883975

- PÉREZ DE LOS COBOS ORIHUEL, Francisco. *Nuevas tecnologías y relación de trabajo*. Valencia: Tirant lo Blanch, 1990.

- PUYOL, Javier. *Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa* [en línea]. Valencia: Tirant lo Blanch, 2015. Disponible en: https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490860434

- QUÍLEZ MORENO, José Mª. "La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores". *Revista Española de Derecho del Trabajo* [en línea]. 2019, núm. 217, pp. 127-152. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7029834

- RED HAT. *¿Qué es la transformación digital?* [en línea]. Disponible en: https://www.redhat.com/es/topics/digital-transformation/what-is-digital-transformation

- RODRÍGUEZ ESCANCIANO, Susana. *Derechos laborales digitales: garantías e interrogantes*. Pamplona: Aranzadi, 2019.

- ROJAS, Elisabeth. *El BYOD, ¿un privilegio o un derecho?* [en línea]. Disponible en: https://www.muycomputerpro.com/2012/06/19/byod-privilegio-derecho

- SÁEZ LARA, Carmen. "Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y las comunicaciones". *Temas Laborales: Revista andaluza de trabajo y binestar social* [en línea]. 2017, núm. 138, pp. 185-221. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6552393

- SERRANO GARCÍA, Juana Mª. *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia.* Albacete: Bormazo, 2019. Pág 9.

- UNIVERSIA ESPAÑA. *El impacto laboral de las TIC en la productividad laboral* [en línea]. Disponible en: https://noticias.universia.es/practicas-empleo/noticia/2016/11/17/1146271/impacto-tic-productividad-laboral.html

- WATTS, Stephen. *Why Bring Your Own Enhancement (BYOE) Is Trending in 2020* [en línea]. Disponible en: https://www.bmc.com/blogs/bring-your-own-enhancement-byoe/

- Constitución Española, de 29 de diciembre de 1978.

- Convenio Colectivo Grupo Axa.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- 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.

- Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19.

- STCo 134/1999, de 15 de julio.

- STCo 213/2002, de 11 de noviembre.

- STCo 241/2012, de 17 de diciembre.

- STS de 17 de diciembre de 2007 (rec. 966/2006).

- STSJ CL 1523/2019, de 8 de abril.

- TEDH, Sentencia 5 de septiembre de 2017.

- TEDH, Sentencia 9 de enero de 2018.