FACULTAD DE DERECHO

EL IMPACTO DE LA DIGITALIZACIÓN EN EL DERECHO DE LA PROTECCIÓN DE DATOS Y LA INTIMIDAD EN EL ÁMBITO LABORAL

Autor: Carlota Arróspide Llorente

5º E-3 A

Área de Derecho Laboral

Tutor: Ana Matorras Díaz-Caneja

Madrid

Junio 2022

RESUMEN

La constante evolución de los medios tecnológicos y su utilización por parte de las empresas para ejercer sus funciones propias del control y supervisión de las prestaciones laborales pueden poner en riesgo los derechos personales de los trabajadores, más específicamente los derechos a la intimidad y a la protección de datos. Por ello, en el presente trabajo de investigación se analizarán diversos dispositivos digitales y las particularidades respecto del control empresarial en cada uno de ellos. De este modo, se presentarán las particularidades de los dispositivos digitales puestos a disposición por el empresario, aportados por el propio trabajador, los dispositivos de videovigilancia, los sistemas de geolocalización, los controles biométricos y el teletrabajo. Por otra parte, el consentimiento y el deber de información se sitúan en el eje central a la hora de realizar el juicio de proporcionalidad para valorar la licitud de cada una de las medidas adoptadas por los empresarios. Para ello, se analizará la regulación establecida por la propia ley en esta materia, las aportaciones de la jurisprudencia y la doctrina, así como las concreciones aportadas por la Agencia General de Protección de Datos. Por último, se recogerán las conclusiones y aportaciones críticas adquiridas tras haber procedido al análisis de los supuestos estudiados en esta materia.

PALABRAS CLAVE

Digitalización, protección de datos, intimidad, control empresarial, Agencia General de Protección de Datos.

ABSTRACT

The constant evolution of technological means and their use by companies to exercise their own functions of control and supervision of labor services can put at risk the personal rights of workers, more specifically the rights to privacy and data protection. For this reason, this research paper will analyze various digital devices and the particularities with respect to corporate control in each of them. Thus, the particularities of the digital devices made available by the employer, provided by the worker himself, video surveillance devices, geolocation systems, biometric controls and teleworking will be presented. On the other hand, consent and the duty to inform are at the center of the judgment of proportionality to assess the lawfulness of each of the measures adopted by employers. To this end, we will analyze the regulation established by the law itself in this area, the contributions of case law and doctrine, as well as the specifics provided by the General Data Protection Agency. Finally, the conclusions and critical contributions acquired after having proceeded to the analysis of the cases studied in this matter will be collected.

KEY WORDS

Digitalization, data protection, privacy, corporate control, General Data Protection Agency.

ÍNDICE

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
BOE	Boletín Oficial del Estado
CE	Constitución Española
	de 27 de abril de 2016 (Reglamento general de protección de datos)
ET	Estatuto de los Trabajadores
FJ	Fundamento Jurídico
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STSJ	Sentencia del Tribunal Superior de Justicia
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos

1. INTRODUCCIÓN

1.1. Justificación de la elección del tema

El presente trabajo de fin de grado ha sido elegido con la finalidad de abordar el impacto que tienen las nuevas tecnologías sobre las relaciones laborales. En concreto, el tema se trata desde el punto de vista de la actual regulación laboral y su necesaria adaptación a la cuarta Revolución Industrial.

Desde una primera aproximación, el núcleo de la transformación digital se encuentra en los individuos, no en la tecnología en sí, pues los medios informáticos únicamente son los instrumentos empleados por los seres humanos para la realización de las tareas[1].

De esta forma, las personas se relacionan entre sí, entre otros medios, a través de las diversas plataformas de redes sociales y mensajerías instantáneas. A nivel laboral, el contexto se asemeja bastante, ya que hacemos uso de las herramientas tecnológicas con el fin de realizar las tareas del día a día.

Además, los efectos de la digitalización sobre el empleo y sobre las nuevas formas de trabajo tienen una trascendencia en la regulación laboral, así como en el funcionamiento de las relaciones laborales, pues la legislación debe ir adaptándose a las nuevas necesidades y requerimientos tanto de los trabajadores como de las empresas que surgen como consecuencia del cambio tecnológico. De este modo, el presente trabajo adopta un enfoque que considera todos los intereses en juego, llegando así a soluciones equilibradas para los diversos conflictos que se plantean. Sin embargo, la revolución digital también puede generar situaciones de conflicto con la legislación actual, provocando ciertos desajustes entre la ley y el nuevo entorno laboral.

Por otro lado, la privacidad de las personas durante las jornadas laborales también se verá amenazada por la digitalización, pues las empresas podrían utilizar los diferentes instrumentos digitales con el fin de controlar y vigilar a los trabajadores, surgiendo así un nuevo reto para proteger de forma apropiada el derecho de intimidad de los empleados y el derecho a la protección de datos, así como la prestación laboral correcta del trabajador.

[1] Slotnisky, D., "Transformación digital: cómo las empresas y los profesionales deben adaptarse a esta revolución", Digital House, Coding School, 2016 p. 3

De este modo, el principal objetivo del trabajo que se presenta es dar a conocer los principales problemas que están surgiendo para los derechos de los trabajadores reconocidos en relación con la digitalización, así como identificar algunos vacíos legales que presenta la regulación actual ante diversos supuestos en relación con las nuevas tecnologías de la información y la comunicación.

2. DIGITALIZACIÓN

2.1 Concepto

La constante evolución de la tecnología ha provocado una nueva realidad laboral plasmada en torno a la digitalización.

La digitalización se puede definir como el proceso de transformar información analógica en un formato digital, facilitando así la manipulación electrónica de los datos. De este modo, la información plasmada en documentos de papel puede ser transformada en imágenes electrónicas o archivos digitales.[2]

Las empresas disponen de diversos métodos para proceder al tratamiento de los datos de los trabajadores con la finalidad de controlar y supervisar la prestación laboral de los empleados como, por ejemplo, a través de los dispositivos electrónicos que ponen a disposición de los mismos, sistemas de videovigilancia, sistemas de geolocalización o, incluso, a través del correo corporativo que utilizan los trabajadores, como veremos detalladamente más adelante.

Todo ello afecta tanto a las formas de trabajo como a la gestión de los recursos humanos. En primer lugar, las formas de trabajo han variado notablemente a través de la implementación de las nuevas tecnologías, como por ejemplo mediante el teletrabajo, es decir, la posibilidad de prestar los servicios desde una localización fuera de las oficinas de la propia empresa.

En segundo lugar, la gestión de los recursos humanos se ha visto afectada por las nuevas tendencias globales recogidas en diversos estudios como el elaborado por el capital humano de Deloitte. En este estudio, se reescriben las reglas para la nueva era digital desde el punto de vista de las personas, las plataformas y el trabajo exponiendo que, como consecuencia de la digitalización total de una compañía, el departamento de recursos humanos debe transformarse "en el líder de la organización digital. Esto implica ir más allá de la digitalización de las plataformas de recursos humanos para desarrollar entornos

[2] Spremolla, G. C., "El trabajo en la era digital", Revista de derecho, 2017, p. 106

y fuerzas laborales digitales, y desplegar tecnología que cambie la manera en que los empleados trabajan y la manera en que se relacionan mutuamente en el trabajo.[3]

Por otro lado, la digitalización es una indudable fuente de oportunidades para las compañías, pues les permite crecer buscando nuevas formas de trabajo más eficientes y transformarse en virtud de la creación de valor para las mismas. Sin embargo, un mal uso de la tecnología "no debidamente controlada y manejada"[4] puede provocar una amenaza para las propias empresas y sus trabajadores.

2.2 Antecedentes

Diversos informes como el elaborado por Spremolla (2017), examinan los cambios que se han generado en el mundo laboral a raíz del continuo avance de la tecnología, más concretamente sobre las nuevas formas de trabajo, formas de organización de las compañías, los modelos de negocio e, incluso, sobre la regulación laboral y las relaciones laborales.

Desde los tradicionales estudios de John Dunlop hasta la actualidad, en el contexto de las relaciones laborales, se ha resaltado la necesidad de observar el entorno tecnológico como una variable independiente apta para dar respuesta a diversas situaciones propias del mundo laboral. Durante las décadas de los 70, 80 y 90, la revisión de la literatura centrada en Relaciones Laborales se caracterizaba por examinar los cambios significativos que se estaban ocasionando durante esa época en el mundo empresarial.

Durante los últimos años, la revolución tecnológica se ha multiplicado de tal forma que surge la necesidad de seguir estudiando el impacto que están produciendo las nuevas tecnologías, primordialmente como una manera de comprender los cambios y adaptaciones que se deberán realizar con el fin de reducir los inconvenientes para los trabajadores, los clientes, o, incluso, para las propias compañías.

[3] Deloitte, "Reescribiendo las reglas para la era de digital. Tendencias Globales en Capital Humano 2017.", Deloitte University Press, 2017, p. 7.
[4] Spremolla, G. C., op. cit., p. 106

3. DERECHOS DEL CIUDADANO RECONOCIDOS EN RELACIÓN CON LA DIGITALIZACIÓN

3.1 Derecho a la intimidad

El derecho a la intimidad se encuentra recogido en el artículo 18.1 y 18.4 de la Constitución Española (en adelante, CE). De este modo, el artículo 18 CE expresa:

> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[5]

Por tanto, el derecho a la intimidad es "irrenunciable, inalienable e imprescriptible."[6] Sin embargo, la propia ley tiene sus limitaciones en los supuestos de autorización por la misma ley o consentimiento expreso por el titular del derecho.

Por otra parte, el derecho de la intimidad puede verse respaldado a través del artículo 4.2 e) del Estatuto de los Trabajadores (en adelante, ET). De este modo, los trabajadores tienen derecho "al respeto de su intimidad y a la consideración debida a su dignidad".[7]

Dentro de la esfera laboral, es frecuente encontrarse con supuestos en los que colisione el control del empresario con el derecho de la intimidad del trabajador, por ello, el Tribunal Constitucional (en adelante, TC) ha defendido en numerosas ocasiones la compatibilidad entre la efectividad de los derechos y libertades fundamentales de los trabajadores y las limitaciones recíprocas que surgen por ambas partes, tanto de la facultad empresarial como de los mismos empleados [8].

Además, el uso de las nuevas tecnologías puede llegar a suponer una vulneración del derecho al respeto de la intimidad. Por ejemplo, cuando intermedian el uso de dispositivos digitales en el ámbito laboral, dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo o la utilización de sistemas de geolocalización en el ámbito laboral.

[5] Artículo 18 de la Constitución Española (BOE núm.311, de 29 de diciembre de 1978). [En adelante, CE]
[6] Artículo 1 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (BOE núm. 115, de 14 de mayo de 1982).
[7] Artículo 4.3 de 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 (BOE núm. 255, de 24 de octubre de 2015). [En adelante, ET]
[8] STC 196/2004, de 15 de noviembre (BOE núm. 306, de 21 de diciembre de 2004).

3.2 Derecho a la protección de datos

El tratamiento de los datos personales debe estar proyectado para servir a la sociedad. Por tanto, el derecho a la protección de datos no se puede comprender como un "derecho absoluto"[9], sino que debe contemplarse en relación con su cometido en la sociedad y salvaguardar el equilibrio con el resto de los derechos fundamentales en función del principio de proporcionalidad.

Por su parte, el derecho a la protección de datos se encuentra recogido en el artículo 18.4 CE que expresa: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."[10] De este modo, se refleja la protección de la ley a los ciudadanos ante el inminente avance de las nuevas tecnologías.

Por otro lado, una de las doctrinas más relevantes en España acerca del derecho de protección de datos ha sido la elaborada por Pérez Luño (1996), donde define este concepto como "un nuevo derecho de autotutela de la propia identidad informática: el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico"[11].

Esta doctrina ha sido acogida por la jurisprudencia del TC, garantizando así la protección de datos como un derecho fundamental. Cabe destacar su primera sentencia al respecto, la STC 254/1993, donde se refiere a este derecho como "libertad informática"[12].

No obstante, no fue considerado como un derecho fundamental autónomo del derecho de la intimidad hasta la STC 292/2000, donde se expresa "el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"[13].

Por otra parte, la STC 292/2000 delimita el objeto y alcance del derecho fundamental de la protección de datos en su fundamento jurídico 6:

[9] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento general de protección de datos, a partir de ahora, RGPD)
[10] Artículo 18.4 CE.
[11] Pérez Luño, A.E., "Manual de informática y derecho". Barcelona: Ariel, 1996, p. 43.
[12] STC 254/1993, de 20 de julio (BOE núm. 197, de 18 de agosto de 1993).
[13] STC 292/2000, de 30 de noviembre (BOE núm. 4, de 04 de enero de 2001).

[…] a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal.[14]

Por tanto, en el ámbito laboral, el empresario deberá respetar cualquier tipo de dato de carácter personal de los trabajadores, tanto aquellos datos que se refieran a la vida privada del trabajador como los datos personales que permanezcan públicos.

3.3 Consentimiento

La STC 292/2000 también define los elementos característicos de este derecho en su Fundamento Jurídico 7 como un derecho a conocer y prestar su consentimiento sobre el almacenamiento y utilización de sus propios datos personales[15].

Por tanto, el derecho a la protección de datos radica en el consentimiento del afectado, es decir, el poder de disposición y control sobre los propios datos personales de un individuo, permitiéndole tomar la decisión acerca de cuáles desea compartir, así como facultándole para tener conocimiento de quiénes poseen sus datos personales, pudiendo en todo momento oponerse a la utilización por terceros.

En referencia al consentimiento de los trabajadores afectados, atenderemos a la Ley Orgánica 3/2018, de 5 de diciembre, referida a la Protección de Datos Personales y garantía de los derechos digitales (a partir de ahora, LOPD), por la que se sustituye a la antigua Ley orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

En el artículo 6.1 de la LOPD, se establece la necesidad de hacer constar dicho consentimiento de forma "específica e inequívoca"[16] para cada una de las finalidades en las que se pretenda fundar el empresario en el ejercicio del tratamiento de datos, salvo que exista legitimación para que los datos puedan ser obtenidos sin el consentimiento.[17]

[14] STC 292/2000, de 30 de noviembre (FJ 6)
[15] STC 292/2000, de 30 de noviembre (FJ 7)
[16] Artículo 6.1 de la Ley Orgánica 3/2018, de 5 de diciembre, referida a la Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018) (a partir de ahora, LOPD).
[17] STC 39/2016, de 3 de marzo (BOE núm. 85, de 08 de abril de 2016). (FJ 3)

En este sentido, la STC 292/2000 en su Fundamento Jurídico 16 define que será el legislador quien especifique en qué casos y en qué circunstancias se justifica la limitación del derecho a la protección de datos.

En el ámbito laboral, el consentimiento por parte de los trabajadores se sitúa en un segundo plano, pues se concibe implícito en la relación laboral, siempre y cuando el tratamiento de los datos personales se requiera para el correcto cumplimiento del contrato laboral[18]. De este modo, la base jurídica de la facultad del empresario radica en el propio contrato de trabajo y las facultades legales de control que dispone el empresario.

Por tanto, según el artículo 20.3 ET, el consentimiento de los trabajadores no será necesario cuando el empresario ejerza las funciones propias de control y supervisión de las prestaciones laborales. Sin embargo, cuando dichas medidas tengan fines ajenos a los servicios propios de la relación contractual entre trabajador y empresario, sí será necesario contar con el consentimiento de forma expresa e inequívoca del trabajador afectado.

3.4 Derecho de información

En la Sección 1 del Capítulo III del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento general de protección de datos y, a partir de ahora, RGPD) se regulan los derechos del interesado en referencia a la transparencia de la información, la comunicación y las diversas modalidades que tienen los interesados para ejercitar sus derechos.

Según el artículo 12 del RGPD el responsable del tratamiento de datos tendrá la obligación de tomar las medidas que considere oportunas con el fin de proporcionar a los interesados toda la información prevista en el presente Reglamento, más concretamente en los artículos 13 y 14 acerca de la información y el acceso a los datos, en los artículos 15 a 22 acerca de los derechos que pueden ejercitar en su defensa, y, finalmente, en el artículo 34 relativa a la comunicación al interesado en caso de violación de la seguridad de los datos personales.

[18] STC 39/2016, de 3 de marzo, (FJ 3)

De este modo, las empresas deberán informar a sus empleados de "forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo"[19].

En cuanto a los requisitos formales de la comunicación, se podrá realizar tanto por escrito como por otros medios, como por ejemplo a través de los medios electrónicos si procede. Además, cuando así lo solicite el trabajador, la información podrá proporcionarse verbalmente siempre y cuando se manifieste la identidad del interesado por otros medios.

Finalmente, la STC 292/2000 también reconoce el derecho a ser informado sobre la posesión de los datos personales y con qué fin por terceros, así como la posibilidad de requerir justificación por la obtención de los mismos.

En conclusión, el derecho a la protección de datos se sitúa como un derecho fundamental independiente del derecho a la intimidad, garantizando a todos los individuos la facultad de disponer y controlar sus propios datos personales y situando el deber de información y el consentimiento como eje central en el ejercicio de este derecho, sin perjuicio de las limitaciones establecidas por el legislador cuando concurran otros derechos que justifiquen dicha restricción.

[19] Artículo 12 del RGPD

4. MARCO LEGAL EN RELACIÓN CON LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

4.1 Dispositivos digitales

4.1.1 Problemática jurídico-laboral asociada a la utilización de dispositivos digitales: comunicaciones y otros posibles usos

Según la Real Academia Española, el correo electrónico se puede definir como un "sistema de transmisión de mensajes por computadora u otro dispositivo electrónico a través de redes informáticas."[20]

Cabe destacar la distinción entre el correo electrónico personal del correo corporativo, pues este último comprende el nombre comercial de una compañía. Entre las ventajas del correo corporativo nos podemos encontrar con una mejoría en la imagen de la empresa y, por otra parte, con la satisfacción de las necesidades de los demandantes a través de una mayor seguridad, velocidad, eficacia a través de la sincronización en varios dispositivos digitales, organización de los contactos y eventos, etc.[21]

Sin embargo, la problemática que se estudia en el presente trabajo traspasa las fronteras del correo electrónico. El uso, tolerado o no, excesivo o no, etc. de los dispositivos digitales facilitados por la empresa puede ser llevado a cabo con otras finalidades fuera de la propia prestación laboral: navegación por internet, acceso y conversaciones en redes sociales y otros sistemas de mensajería instantánea, realización de gestiones privadas y/o compras online, almacenamiento de toda clase de ficheros personales (texto, vídeo, audio, etc).

De este modo, el control de uso de dispositivos por parte de la empresa puede llegar a invadir esos otros espacios y actuaciones que pueden comprometer más aún la intimidad o el derecho a la protección de datos.

Por ello, en el presente trabajo se diferencian los supuestos en los que el empleado utiliza herramientas y medios digitales facilitados por la empresa con fines laborales, respecto de los supuestos de utilización de medios propios, e incluso los supuestos en los que las

[20] Real Academia Española. Disponible en https://dle.rae.es/ ; última consulta el 5/03/2022.
[21] Tortosa Miralles, J. A., "El uso del correo electrónico en el trabajo", Universitat Jaume I, 2016, p. 5. Disponible en http://repositori.uji.es/xmlui/handle/10234/164466 ; última consulta el 5/03/2022.

empresas facilitan dispositivos para un uso mixto, que habrá de estar bien acotado y separado a efectos de ejercicio de facultades de control.

4.1.2 Facultad empresarial de controlar el uso de los dispositivos digitales facilitados por la empresa

El artículo 87 de LOPD protege el derecho a la intimidad de los trabajadores frente al uso de dispositivos digitales puestos a su disposición por la empresa.

Respecto al poder empresarial en esta materia, en virtud del artículo 87.2 LOPD, se reconoce la facultad de la empresa para acceder a los diferentes contenidos procedentes de la utilización de los dispositivos digitales facilitados a los trabajadores "a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos." [22]

Más adelante, el artículo 87.3 LOPD exige a las empresas concretar los criterios de utilización de los medios digitales cumpliendo siempre "los estándares mínimos de protección de su intimidad"[23] previstos tanto constitucional como legalmente, determinando así una obligación que todo empleador deberá cumplir. Asimismo, con el fin de evitar que los criterios mencionados se dejen al arbitrio del empresario, en su elaboración deberán intervenir los representantes de los trabajadores.

Además, se reconoce el derecho de los trabajadores a ser informados de los criterios de uso de los dispositivos digitales llevados a cabo por la empresa. Sin embargo, parte de la doctrina defiende que el legislador debería haber aprovechado para detallar los mecanismos o controles de inspección que se llevarán a cabo por la empresa con el fin de fiscalizar el uso apropiado de los dispositivos digitales conforme a los criterios previstos en la ley en vez de limitarse a informar sobre dichos criterios.[24]

Respecto a los supuestos en los que las empresas facilitan dispositivos para un uso mixto, el acceso de la empresa a los contenidos generados por los medios digitales de los que se ha permitido su utilización para fines privados han de cumplir con el artículo 87.3 LOPD. Así, el citado artículo exige que se concreten los usos autorizados de forma precisa y se

[22] Artículo 87.2 LOPD.
[23] Artículo 87.3 LOPD.
[24] Quílez Moreno J. M., "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 num. 217/2019, p.24.

establezcan las garantías para salvaguardar la intimidad de los trabajadores, como, por ejemplo, la fijación de los períodos determinados en los que dichos dispositivos podrán usarse para fines privados.

Además, el artículo 20.3 ET también se ha pronunciado sobre las facultades empresariales de dirección y de control de la actividad laboral. Respetando siempre la dignidad de los trabajadores, cabría afirmar que la empresa se encuentra facultada para adoptar las medidas que considere "más oportunas"[25] con el fin de supervisar y controlar a sus empleados dentro del ámbito laboral, asegurándose así el correcto cumplimiento de los deberes y obligaciones laborales de los trabajadores.

Por otra parte, se introduce el artículo 20 bis ET a través de la disposición final decimotercera de la LOPD. Este artículo hace alusión directa al uso de los dispositivos de digitales puestos a disposición del trabajador por la propia empresa, tratando así de proteger los derechos a la intimidad de los trabajadores en relación con el entorno digital.

Por ello, los empresarios deberán determinar e informar acerca de los criterios de uso de los medios digitales que ponen a disposición de los trabajadores, así como de las políticas internas que traten de salvaguardar el derecho de desconexión digital de los empleados fuera de sus jornadas laborales.[26]

En la STC 170/2013, de 7 de octubre de 2013 (Recurso de amparo 2907-2011), se corrobora que el uso extralaboral del correo corporativo, es decir, del correo electrónico proporcionado por la empresa, no supone una vulneración del derecho a la intimidad ni al secreto de las comunicaciones. De este modo, la sentencia expone en su Fundamento Jurídico 4 que la prohibición convencional de forma expresa de la utilización extralaboral del correo corporativo faculta a la empresa para controlar su uso de forma implícita con el fin de supervisar el cumplimiento de las prestaciones laborales.[27]

De este modo, el correo corporativo se encuentra dentro de la esfera de la propiedad del empresario, pudiendo hacer uso del mismo y presentarlo como prueba ante un despido

[25] Artículo 20.3 ET.
[26] Sánchez-Ostiz, J. C., y Sancha, J. F., "Novedades en el ámbito laboral de la nueva Ley Orgánica de Protección de Datos". Actualidad Jurídica Aranzadi, 2018, p.1.
[27] STC 170/2013, de 7 de octubre de 2013 (Recurso de amparo 2907-2011). (BOE núm. 267, de 7 de noviembre de 2013).

por utilizarlo con otros fines que no sea la actividad empresarial para la que ha sido puesto en disposición del trabajador.

No obstante, en el caso de la STC 170/2013, de 7 de octubre de 2013, cabe destacar la naturaleza convencional de esta prohibición, pues, en virtud de lo determinado en el artículo 82.3 ET acerca de las regulaciones colectivamente pactadas, se permite tipificar como una infracción sancionable por el empresario el uso del correo electrónico de propiedad empresarial para fines ajenos al objeto de la prestación laboral. De este modo, el trabajador estaba plenamente informado acerca de las consecuencias que podría tener el hecho de hacer un mal uso del correo corporativo.

4.1.3 Limitaciones

En referencia a las comunicaciones electrónicas en la esfera de las relaciones laborales, la STC 241/2012 indica en su Fundamento Jurídico 5 que las empresas tienen potestad para regular la utilización de los medios informáticos que ponen a disposición de los empleados, así como la capacidad para vigilar y controlar el cumplimiento de las obligaciones que nacen en torno a los dispositivos digitales, sin perjuicio del absoluto respeto a los derechos fundamentales de los trabajadores. Aquí encontramos la primera limitación del control y vigilancia del uso del correo corporativo por parte del empresario.

No obstante, la mencionada STC 241/2012 precisa un matiz a la limitación de los derechos fundamentales, teniendo en consideración "los grados de intensidad o rigidez" a la hora de valorar las medidas adoptadas por el empresario, pues varían en función de la propia naturaleza de las condiciones de uso y disposición de los medios informáticos, así como de las instrucciones que haya proporcionado el mismo empresario a sus trabajadores.

De este modo, se establece el principio de proporcionalidad a la hora de valorar la licitud del control empresarial a través de cuatro factores distintos. En primer lugar, la idoneidad, donde la limitación de los derechos del trabajador debe ir dirigida para conocer el uso que están realizando de los dispositivos electrónicos respecto a las prestaciones laborales. De este modo, debe concurrir una adecuación entre la conducta del empresario y los fines que se pretenden alcanzar. En segundo lugar, la necesidad, pues, dentro de todas las medidas que puede adoptar el empresario, se debe adoptar la más moderada que consiga la misma eficacia. De esta forma, se lesiona lo mínimo posible los derechos

fundamentales de los trabajadores. En tercer lugar, la justificación, pues siempre deberán responder ante razonamientos y motivos objetivos, sin mediar ninguna conveniencia o arbitrariedad por parte del empleador. Por último, se procederá a una ponderación, es decir, una puesta en equivalencia entre las ventajas que proporciona esa medida para el interés general sobre las desventajas y perjuicios que genera sobre otros bienes o derechos del trabajador. De esta manera, se garantiza un equilibrio entre la lesión que se provoca a los trabajadores y el interés del empresario que se pretende proteger.[28]

La jurisprudencia del TDEH pone de manifiesto el juicio de proporcionalidad a través del análisis de cinco factores: el grado de intrusión de la empresa, la existencia de una razón justificada y legítima acerca de la medida adoptada por la empresa, la existencia o no de otros medios que resulten menos intrusivos para alcanzar el mismo fin, el destino perseguido por la empresa y las garantías previstas para el empleado.[29]

La jurisprudencia del TS y TSJ también han hecho uso del juicio de proporcionalidad mencionado con el fin de analizar la ponderación de intereses y el equilibrio entre los derechos de los trabajadores y los intereses del empresario. Como, por ejemplo, la STSJ de Catilla-La Mancha en su sentencia núm. 515/2021 de 25 marzo.

Por tanto, en las relaciones laborales, el control del empresario del correo proporcionado por la misma no supone ninguna vulneración al derecho de intimidad o al secreto de comunicaciones, siempre que el trabajador se encuentre informado, que respete los derechos fundamentales y que cumpla el principio de proporcionalidad bajo los criterios de idoneidad, necesidad, justificación y ponderación.

Por otra parte, con el fin de examinar la regulación de la facultad del empresario a nivel internacional, atenderemos al Capítulo II del RGPD donde se encuentran los principios relativos al tratamiento de datos personales, más concretamente en el artículo 5.1. Sin embargo, cabe destacar que el RGPD no ha diferenciado su aplicación respecto de los múltiples dispositivos que pueden afectar al derecho de la intimidad y protección de datos de los trabajadores, planteando así una gran problemática a la hora de abordar los casos en la práctica.

[28] Tortosa Miralles, J. A., op. cit., p. 7.
[29] STSJ Castilla-La Mancha, (Sala de lo Social, Sección2ª) Sentencia núm. 515/2021 de 25 marzo. FJ 5

En primer lugar, se determina que los datos personales deberán ser "tratados de manera lícita, leal y transparente"[30]. De este modo, aparece la obligación del empresario de cumplir con los principios de licitud, lealtad y transparencia. En referencia a este último principio, ya se ha analizado en el apartado anterior la exigencia de proporcionar toda la información, así como de los requisitos de la facilidad del acceso y comprensión por parte del interesado.

En segundo lugar, se regula el principio de la limitación de la finalidad del tratamiento de los datos personales, que deberán ser obtenidos "con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"[31]. Respecto al tratamiento ulterior de los datos personales, cabe destacar que, según el artículo 89 RGPD, no se considerarán incompatibles los tratamientos con fines de archivo en virtud del interés público, fines de investigación científica o histórica, ni cuando se trate de fines estadísticos.

En tercer lugar, se expone el principio de minimización de datos, pues deberán ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"[32].

Además, el RGPD también hace mención del principio de proporcionalidad en el derecho de la protección de datos, tomando así un papel esencial a la hora de determinar la legitimación de las medidas adoptadas por el empresario.

En cuarto lugar, se regula el principio de exactitud. De este modo, los datos personales obtenidos por parte del empresario deberán ser exactos, y, si procede, actualizados, adoptando así todas las medidas que se consideren oportunidad con el fin de eliminar o rectificar sin dilación los datos inexactos respecto al fin que se pretende.

En quinto lugar, se establece una limitación del plazo de conservación de los datos personales, que deberán ser conservados de manera que no se admita identificar a los interesados más del tiempo requerido para alcanzar la finalidad perseguida [33]. No obstante, se permite ampliar el plazo en los casos previstos en el artículo 89 RGPD

[30] Artículo 5.1 RGPD
[31] Artículo 5.1 RGPD, op. cit.
[32] Artículo 5.1 RGPD, op. cit.
[33] Artículo 5.1 RGPD, op. cit

mencionado anteriormente, sin perjuicio de la adopción de las medidas técnicas y organizativas para proteger los derechos y libertades del interesado.

De nuevo, la ley no determina un plazo específico para el tratamiento de los datos personales de los trabajadores, exponiéndoles así a una generalidad de supuestos que no se encuentran regulados.

Por último, el tratamiento de los datos personales se deberá realizar garantizando una seguridad adecuada, protegiendo así a los interesados en casos de tratamiento ilícito o no autorizado y en casos de pérdida, daño accidental o destrucción a través de la adopción de medidas técnicas y organizativas. De este modo, se contemplan los principios de integridad y confidencialidad.

En conclusión, en virtud del artículo 5.1 del RGPD se consagran los límites de la facultad empresarial en torno a los dispositivos digitales a través de los principios de licitud, lealtad, transparencia, limitación de la finalidad del tratamiento, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad, y, finalmente, el principio de proporcionalidad. De este modo, los datos recabados a partir de los dispositivos digitales que no cumplan los principios mencionados no podrán ser objeto de tratamiento por parte del empresario.

Por otro lado, en el ámbito de la Unión Europea cabe destacar la sentencia del Tribunal Europeo de Derechos Humanos (en adelante, STEDH) de 3 de abril de 2007 en el asunto Copland contra Reino Unido, se pronuncia acerca de las normas de uso de los dispositivos electrónicos que la empresa pone a disposición de los trabajadores, así como de las posibles prohibiciones y limitaciones de uso privado.

La STEDH establece el derecho del respeto de la vida privada y familiar como límite al control y vigilancia empresarial. En este caso, las comunicaciones telefónicas, los mensajes enviados a través del correo electrónico y la navegación por internet de la demandante, la Sra. Lynette Copland, habían sido interceptados por el empresario. En la demanda se alegaba una vulneración de su derecho al respeto de la vida privada y familiar, amparándose bajo los artículos 8 y 13 del Convenio para la Protección de los Derechos Humanos y de las Libertades Públicas.

El Tribunal Europeo de Derechos Humanos (en adelante, TEDH), hace especial referencia al conocimiento por parte de la trabajadora, ya que si la demandante hubiese estado correctamente informada por parte del empresario, la interferencia en sus datos de carácter personal a través del teléfono, del correo electrónico y de internet no hubiesen incurrido en una vulneración de su derecho al respeto de su vida privada.

Por otra parte, el Gobierno británico defiende que la ley permitía al centro educativo donde trabajaba la demandante la adopción de "todas las medidas útiles y necesarias"[34] para el correcto cumplimiento de su prestación laboral. Sin embargo, el Gobierno británico no alegó ninguna ley en la que previesen los casos en el que los empresarios pudiesen controlar el uso de los dispositivos electrónicos de sus empleados.

En resumen, la STEDH de 3 de abril de 2007, reconoce la facultad del empresario para vigilar y controlar los medios informáticos, pero a su vez exige que tenga un fin legítimo y que la medida se encuentre prevista por ley, de modo que los trabajadores puedan llegar a conocer con exactitud en qué situaciones y condiciones pueden las empresas adoptar estas medidas y puedan prescindir de las expectativas de privacidad en sus comunicaciones.

Finalmente, la STEDH concluyó que la empresa no se encontraba amparada bajo ninguna ley y, además, tampoco había comunicado a la demandante que sus comunicaciones eran susceptibles de ser interceptadas. Por tanto, se produjo una vulneración del artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, constituyendo así una injerencia en el derecho al respeto de la vida privada de la demandante.

En el caso de la STC núm. 170/2013 de 7 de octubre (RTC 2013, 170), el hecho de que el uso extralaboral de los medios informáticos puestos a disposición del trabajador estuviese tipificado como una infracción sancionable a través del Convenio colectivo establece una importante particularidad frente a algunos de los supuestos enjuiciados por el TDEH, como el expuesto anteriormente. La razón radica en que la tipificación en los

[34] STDH de 3 de abril de 2007, asunto Copland contra Reino Unido, núm. 62617/00. Disponible en https://www.mjusticia.gob.es/es/AreaInternacional/TribunalEuropeo/Documents/1292429139374-Trad._Sentencia_COPLAND_c.REINO_UNIDO.pdf ; última consulta el 6/03/2022.

Convenios colectivos elimina cualquier expectativa de los trabajadores de privacidad en los dispositivos digitales puestos a su disposición.

Por otro lado, varios autores, como Sempere Navarro y San Martín Mazzucconi han resaltado las limitaciones que presenta la ley en este asunto, "dada la constante evolución tecnológica y el riesgo de que los preceptos normativos queden obsoletos"[35].

Por tanto, según Pérez de los Cobos Orihuel y García Rubio, se presume que la doctrina actual ni termine con las controversias en la abundante casuística que puede llegar a presentarse en este ámbito, ni tampoco agote la necesidad existente de contar con una normativa que regule el equilibrio entre los derechos y libertades afectadas, con la finalidad de aportar una mayor seguridad jurídica. Se reivindica así "el papel protagonista"[36] del legislador en esta materia.

En resumen, es casi seguro que, en mayor o en menor medida, en el futuro nuestros Tribunales se enfrenten con nuevas problemáticas a la hora de abordar el control empresarial ante las comunicaciones electrónicas en el ámbito laboral. De este modo, la jurisprudencia se irá adaptando y completando pues parece ser que aún se encuentra en fase de construcción.

Por último, cabe destacar la repercusión penal del control empresarial del correo electrónico a través de la doctrina jurisprudencial. En primer lugar, en la STS núm. 528/2014, de 16 de junio, el acceso de la empresa a los correos que no hubiesen sido leídos previamente por el trabajador necesitaba previa autorización judicial al suponer una vulneración del derecho al secreto de las comunicaciones[37]. No obstante, en la STS núm. 489/2018, de 23 de octubre, se disminuye la relevancia al hecho de que los correos electrónicos se encontrasen leídos o no, pues lo verdaderamente importante se encontraba en la expectativa de privacidad por parte del trabajador[38]. Por tanto, la expectativa de confidencialidad es lo que diferenciará una medida legítima de otra ilegítima, cabiendo matizar que "la exclusión de esa expectativa ha de ser expresa y consciente, sin que pueda

[35] Pérez de los Cobos Orihuel F. y García Rubio M. A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos.", Revista Española de Derecho del Trabajo num. 196/2017, 2017, p. 13

[36] Pérez de los Cobos Orihuel F. y García Rubio M. A., op. cit., p. 13

[37] STS núm. 528/2014, de 16 de junio.

[38] STS núm. 489/2018, de 23 de octubre.

equipararse a ésta una pretendida renuncia derivada de la voluntad presunta del trabajador"[39].

4.1.4 Derechos digitales en la negociación colectiva

En virtud del artículo 91 LOPD, los convenios colectivos pueden determinar diferentes garantías adicionales acerca de la protección de los datos personales, así como de la protección de los derechos digitales en el ámbito laboral.

Un ejemplo de ello sería el Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones aprobado en septiembre de 2021. En su artículo 37.1 expone la facultad empresarial para acceder a los dispositivos digitales puestos a disposición de los trabajadores con el fin de supervisar el correcto cumplimiento de las obligaciones tanto laborales como estatutarias.[40]

De este modo, se observa la imposibilidad de los trabajadores para hacer un uso personal de los dispositivos electrónicos puestos a su disposición y, por otro lado, la facultad empresarial para acceder al contenido con la finalidad de ejercer las funciones propias de control de la prestación laboral.

Por otro lado, el Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal del 29 de diciembre de 2021, dedica su artículo 119 para regular el derecho a la intimidad frente al uso de los dispositivos digitales. En el citado artículo, se faculta al empresario para acceder a los contenidos de los dispositivos digitales que el empresario pone a disposición de los trabajadores con la finalidad de controlar el cumplimiento de las obligaciones tanto laborales como estatutarias, así como de proteger la integridad de los propios dispositivos.

Además, el Convenio colectivo anterior establece una nueva obligación con el fin de salvaguardar en mayor medida los estándares mínimos de protección de la intimidad de los trabajadores, donde el empresario deberá determinar los criterios del uso de los medios

[39] Elizalde Purroy I. "España | ¿Posible delito por acceso al ordenador y al correo electrónico del trabajador/a?", Cuatrecasas, 1 de junio de 2021. Disponible en https://www.cuatrecasas.com/es/spain/articulo/puede-constituir-delito-acceso-ordenador-correo-electronico-persona-trabajadora ; última consulta el 31/05/2022.

[40] Artículo 37.1. Resolución de 3 de septiembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones.

digitales "con la participación de la representación legal de los trabajadores"[41]. Seguidamente, el Convenio colectivo delimita de forma concreta el procedimiento para identificar los criterios a seguir por la empresa, donde el empresario quedará obligado a formalizar a través de "una normativa interna" tanto el acceso a los diversos sistemas como el uso del correo corporativo, el almacenamiento de los datos o la instalación de programas.[42]

Por último, el Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal también regula el acceso de la empresa al contenido de los dispositivos digitales que se hubiesen permitido su uso para fines privados.

En estos casos, se deberá especificar de manera precisa los usos autorizados así como las garantías oportunas para proteger la intimidad de los trabajadores como, por ejemplo, la especificación de los períodos en los que los trabajadores pueden utilizar los dispositivos puestos a su disposición para fines privados.

No obstante, algunos convenios colectivos como por ejemplo el Convenio colectivo de Teleinformática y Comunicaciones del 11 de junio de 2020 o el de Telefónica Ingeniería de Seguridad del 23 de diciembre de 2019, se limitan a señalar que el artículo 20 bis ET reconoce de manera bastante "amplia y genérica"[43] el derecho a la intimidad de los trabajadores frente al uso de los dispositivos digitales, de videovigilancia y de geolocalización, "dejando un amplio margen de libertad a las partes para proceder a su regulación."[44]

En resumen, a pesar de las lagunas legales que se presentan en la regulación del derecho de la intimidad de los trabajadores frente a los dispositivos digitales, se puede comprobar cómo los convenios colectivos cada vez van especificando más el uso de los dispositivos digitales con el fin de salvaguardar los derechos digitales de los trabajadores.

[41] Artículo 119. Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal.
[42] Artículo 119. Resolución de 29 de diciembre de 2021, op. cit.
[43] Artículo 27. Resolución de 11 de junio de 2020, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Teleinformática y Comunicaciones, SAU
[44] Artículo 41. Resolución de 23 de diciembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Telefónica Ingeniería de Seguridad SAU.

4.1.5 Facultad empresarial de controlar los dispositivos digitales aportados por el trabajador

Cada vez más empresas deciden implantar la práctica denominada *bring your own device*, donde los trabajadores hacen uso de sus propios medios informáticos como sus ordenadores o teléfonos para desarrollar las prestaciones laborales.

Cabe destacar el vacío legal en la regulación de estos supuestos, pues, en una primera instancia, no se encuentran amparados bajo el artículo 20.3 ET a través del cual se faculta al empresario para controlar el cumplimiento de las prestaciones laborales de los dispositivos puestos a disposición de los trabajadores.

Por tanto, en un principio nos encontraríamos bajo el artículo 18 ET, donde se expresa la inviolabilidad de la persona del trabajador. Según este artículo, únicamente se podrá registrar en los efectos particulares del trabajador cuando se requiera para proteger tanto el patrimonio de la empresa como el del resto de empleados[45]. Además, se establece la obligación de realizarlos dentro de la jornada laboral y en el centro de trabajo.

Arrivasplata Reyes compara la monitorización de los equipos informáticos proporcionados por el empresario respecto de los dispositivos personales de los trabajadores para desarrollar las prestaciones laborales. Así, la jurista defiende la inexistencia de ninguna "razón objetiva"[46] que imposibilite extender la regulación legal de los dispositivos puestos a disposición por la empresa a los supuestos en que el control empresarial se lleve a cabo en el propio ordenador o teléfono móvil del trabajador.

Asimismo, parte de la doctrina asemeja ambos supuestos sin mencionar las particularidades que tienen los dispositivos personales del trabajador. Por ejemplo, Espuga Torné se limita a expresar el deber de informar a los empleados acerca de las restricciones en el uso permitido[47] sin apreciar ninguna diferencia entre los dispositivos proporcionados por la empresa y los aportados por el propio trabajador.

---

[45] Artículo 18 ET

[46] Arrivasplata Reyes, F. D., "Monitorización de la navegación en internet en el «BYOD»: exigencias del empleador en el marco de la ley de protección de datos personales", *SPDTSS*, 2021, p. 845.

[47] Espuga Torné, G., "La actual situación de emergencia sanitaria causada por la pandemia global de la COVID-19 ha provocado un cambio de paradigma en la organización y realización del trabajo. Este cambio de modelo, basado en el teletrabajo, al que han llegado mejor preparadas las empresas con un alto grado de digitalización, está llamado a permanecer una vez superada la pandemia", *Thomson Reuters*, 24 de

No obstante, en mi opinión habría que tener en cuenta las particularidades de la práctica *Bring your own device* pues nos encontramos ante una conflictividad en expansión y creciente en distintas dimensiones.

Ante la ausencia de una regulación específica y concreta sobre esta materia, la Agencia Española de Protección de Datos (a partir de ahora, AEPD) ha elaborado una serie de recomendaciones para proteger los datos personales de los trabajadores cuando aporten sus dispositivos personales para desarrollar la prestación laboral, donde se define que se deberá evitar el uso personal y profesional de forma simultánea, así como la elaboración de perfiles distintos e independientes para realizar cada tarea. Además, no se deberá hacer uso de las aplicaciones que no se encuentren autorizadas por la empresa para compartir la información profesional, ya sea en los correos personales, servicios en nube de almacenamiento de datos, o cualquier medio de mensajería rápida.[48]

Bien es verdad que la única responsable de aplicar la normativa prevista tanto en la LOPD como en el RGPD es la empresa, "incluyendo los dispositivos privados que se usen para trabajar"[49]. Por ello, es inevitable que el empresario realice ciertas medidas de "control sobre los equipos privados"[50] que los trabajadores utilicen para desempeñar sus prestaciones laborales, aplicando así las garantías de protección previstas en la legislación vigente. Para ello, será preciso cumplir con las recomendaciones mencionadas de la AEPD, más específicamente con la plena división entre los datos privados y de la empresa.

Según Andrés Ricart, los dispositivos aportados por el trabajador que posean acceso a los datos personales de la empresa deberán someterse bajo las mismas medidas de control que el resto de los dispositivos proporcionados por la empresa con el fin de favorecer el correcto cumplimiento de la normativa relativa a la protección de datos.[51]

---

junio de 2020. Disponible en https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/teletrabajo-y-derecho-a-la-desconexion-digital-en-al-ambito-laboral-en-tiempos-de-covid-19-2020-06-24/ ; última consulta el 22/05/2022.

[48] La Agencia Española de Protección de Datos (a partir de ahora, AEPD). "Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo", 2020, p. 6.

[49] Grupo Atico34, "El fenómeno BYOD y la protección de datos", Grupo Atico34, 2020

[50] Grupo Atico34, op. cit.

[51] Andrés Ricart G. "Recomendaciones para el teletrabajo", Thomson Reuters, 24 de junio de 2020. Disponible en https://www.legaltoday.com/colaborador/andres-ricart/ ; última consulta el 24/05/2022.

Según mi punto de vista, dada la ausencia de legislación vigente y la falta de doctrina jurisprudencial precedente que verse sobre la práctica del *bring your own device*, los dispositivos aportados por los empleados para trabajar se dividirán en dos perfiles. Por una parte, en un perfil personal regulado por el artículo 18 ET integrado dentro de los efectos personales del trabajador y, por otra parte, en un perfil profesional donde el empresario podrá controlar, por ejemplo, el correo corporativo proporcionado por la misma desde el servidor de la empresa y sin necesidad de acceder de forma directa al ordenador del trabajador. Un ejemplo de ello sería el reflejado en la sentencia del Juzgado de lo Social núm. 2 de Madrid, sentencia núm. 93/2019 de 12 febrero, aunque en esta misma sentencia el control empresarial no superó el juicio de proporcionalidad al no tomar la medida menos intrusiva para el trabajador y al excederse de forma exponencial en el tiempo[52].

4.2 Dispositivos de videovigilancia en el lugar de trabajo

4.2.1 Concepto de videovigilancia

Según la Real Academia Española, el concepto de videovigilancia se puede definir como la "vigilancia por medio de un sistema de cámaras, fijas o móviles".[53]

En la actualidad, las legislaciones de los distintos Estados no prohíben de forma absoluta la aplicación de los dispositivos electrónicos de vigilancia en el ámbito laboral, incluso en los Estados que poseen una fuerte cultura de protección del derecho de la intimidad en el lugar de trabajo. De este modo, el Derecho trata de mantener un equilibrio entre los intereses de los trabajadores en salvaguardar su privacidad y la justificación de la empresa para tomar medidas que impliquen una vigilancia en el lugar de trabajo.[54]

[52] Sentencia del Juzgado de lo Social núm. 2 de Madrid, sentencia núm. 93/2019 de 12 febrero.
[53] Real Academia Española. Disponible en https://dle.rae.es/ ; última consulta el 5/03/2022.
[54] Agustina Sanllehí, J. R., "Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia", Revista Electrónica de Ciencia Penal y Criminología, 2009, p. 10: 12.

4.2.2 Facultad empresarial de control

En virtud del artículo 38 CE, se garantiza la "libertad de empresa en el marco de la economía de mercado"[55]. De este modo, se protege y defiende su ejercicio, así como la propia productividad de la empresa, sin perjuicio de las diversas exigencias de la economía general.

Conjuntamente, como hemos visto, el artículo 20.3 ET también faculta a la empresa para adoptar las medidas que considere más adecuadas y oportunas con el fin de supervisar el cumplimiento de las prestaciones laborales.

Por otra parte, se produce una modificación del Estatuto de Trabajadores a través de la nueva LOPD. De este modo, se reconoce el derecho a la intimidad de los trabajadores frente al uso de dispositivos de videovigilancia por parte de la empresa.

En definitiva, la facultad del empresario para controlar a sus trabajadores a través de dispositivos de videovigilancia queda sujeta a la obligación de tomar las medidas más respetuosas con los derechos fundamentales de sus empleados. Además, también deberá "circunscribir esta actividad a la comprobación de aquellas cuestiones estrictamente vinculadas con la prestación de trabajo"[56].

Por otro lado, a través del artículo 22 de la LOPD se regula el tratamiento de datos con fines de videovigilancia ante los vacíos legales que está provocando el significativo aumento de las instalaciones de los sistemas de videocámaras. A través del citado artículo se faculta a las personas físicas o jurídicas, ya sean públicas o privadas, para proceder al tratamiento de las imágenes captadas mediando los sistemas de cámaras o videocámaras "con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones"[57]. De este modo, podemos observar que la LOPD enfatiza en un primer momento las funciones de seguridad y bienestar de las personas e infraestructuras.

[55] Artículo 38 CE.
[56] Ballesteros, I. J. C., "Videovigilancia laboral y derecho fundamental a la protección de datos", Revista andaluza de trabajo y bienestar social, núm. 136, 2017, p. 131
[57] Artículo 22.1 LOPD

No obstante, el artículo 22.8 LOPD hace referencia al tratamiento de los datos obtenidos a través de sistemas de videocámaras por parte del empleador, remitiéndolo así al artículo 89 de esta misma ley orgánica.

Por tanto, respecto al uso de las imágenes obtenidas a través de los sistemas de videovigilancia por parte de un empleador, deberemos acudir al artículo 89 de la LOPD, donde se establece el derecho de las empresas para ejercer sus funciones propias de la dirección y supervisión haciendo uso de las imágenes grabadas. Sin embargo, el poder de la empresa quedará limitado al marco legal, así como a los límites y derechos inherentes al mismo.

Por último, el artículo 89 delimita un límite territorial al control empresarial, pues se prohíbe la instalación de sistemas de videovigilancia en las zonas "destinadas al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos".[58]

4.2.3 Derecho de información

Anteriormente, la Instrucción 1/2006, de 8 de noviembre, de la AEPD, regulaba el tratamiento de los datos personales de los trabajadores a través de la obligación por parte de los empresarios de colocar un "distintivo informativo"[59] con el fin de cumplir con el deber de información.

Sin embargo, la propia AEPD establece que desde el 25 de mayo de 2018 la mayor parte de la Instrucción 1/2006 ha quedado desplazada como consecuencia de la aplicación del RGPD.[60]

En primer lugar, la empresa deberá cumplir con el deber de información mencionado en la parte general introductoria sobre el derecho de protección de datos y de la intimidad conforme al artículo 12 del RGPD

Por otro lado, el artículo 22.4 de la LOPD hace referencia al deber de información en los tratamientos de datos con fines de videovigilancia previsto en el artículo 12 del RGPD.

[58] Artículo 89 LOPD

[59] Artículo 3 de la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. («BOE» núm. 296, de 12 de diciembre de 2006)

[60] AEPD. "Guía sobre el uso de videocámaras para seguridad y otras finalidades", 2021, p.24

Según la LOPD, el deber de información se cumple a través de la colocación de un "dispositivo informativo en un lugar suficientemente visible"[61]. Además, se deberá identificar como mínimo la existencia del tratamiento de datos, la identidad del responsable y, por último, la facultad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD. Opcionalmente se podrá incluir un código que permita dirigirse a los afectados directamente a la información contenida en internet. Así, las empresas, como responsables del tratamiento de datos, deberán facilitar a sus empleados toda la información prevista en el RGPD.

Continuando con la LOPD, el artículo 89 también regula el deber de información de forma "expresa, clara y concisa"[62] a los trabajadores y, en su caso, a sus representantes con carácter previo. Sin embargo, el mismo artículo define que en los supuestos en los que intermedie "la comisión flagrante de un acto ilícito"[63] por parte de los empleados únicamente se requerirá la colocación del dispositivo informativo del artículo 22.4 de la LOPD para que el derecho de información se conciba cumplido. De esta forma, vemos como el dispositivo informativo prevalece en los casos de fraude o dolo por parte de los trabajadores.

En resumen, los empresarios que decidan instalar sistemas de videovigilancia en el lugar de trabajo deberán cumplir con el deber de información previsto tanto en el RGPD como en la LOPD. De este modo, las empresas deberán colocar un dispositivo informativo en los lugares videovigilados, tanto los espacios abiertos como en las zonas cerradas. Además, deberán estar ubicados de tal forma que sean suficientemente visibles.

No obstante, parte de la doctrina ha expresado que, para que la cláusula informativa opere con la máxima eficacia, sería preciso que se incluyese dentro del contrato de trabajo.[64]

Respecto a la jurisprudencia, cabe destacar la STC 39/1016, de 3 de marzo, donde se introduce una modificación en el derecho de información, pues se sustituye el deber de información previo a los trabajadores por la instalación visible del dispositivo informativo mencionado en el artículo 22.4 de la LOPD.

[61] Artículo 22.4 LOPD
[62] Artículo 89 LOPD
[63] Artículo 89 LOPD
[64] Quílez Moreno J. M., op. cit., p.24.

En este caso, la empresa, tras haber instalado un nuevo sistema de control en la caja, se percató de numerosas irregularidades en la caja de la tienda donde la demandante prestaba sus servicios. Como consecuencia, la empresa instaló una cámara de videovigilancia con el fin de controlar la caja donde la demandante trabajaba. La instalación se produjo sin previa comunicación a los trabajadores. Sin embargo, en el escaparate de la tienda, es decir, en un lugar claramente visible, se situó el distintivo informativo.

Posteriormente, en 2012, la demandante fue despedida disciplinariamente por violación de la buena fe contractual al haber aparecido en las cámaras apropiándose de forma indebida el dinero de la caja.

Como se ha mencionado al explicar el consentimiento respecto del derecho a la protección de datos, la STC 39/2016 exime al empresario de contar con el previo consentimiento del trabajador en el tratamiento de los datos necesarios para el mantenimiento de la relación laboral, es decir, el cumplimiento de las obligaciones laborales que se derivan del contrato de trabajo.

De este modo, la STC 39/2016 concluye que la empresa no necesita el consentimiento de forma expresa por parte del trabajador en relación con la obtención de datos a través de la instalación de los sistemas de videovigilancia en el lugar de trabajo. La justificación de su decisión radica en la finalidad de seguridad y control del cumplimiento de la relación laboral.

Además, la STC 39/2016 también se basa en su conformidad con el artículo 20.3 ET donde se faculta a la empresa para adoptar las medidas que considere "más oportunas de vigilancia y control"[65] con el fin de supervisar el cumplimiento de las obligaciones laborales.

No obstante, aunque en este caso no fuese necesario contar con el consentimiento de la demandante, el deber de información continúa existiendo, pues en virtud de este deber los trabajadores pueden ejercer su derecho a la protección de datos, es decir, el derecho de acceder, rectificar, cancelar, oponer y conocer al responsable del tratamiento mencionados en a lo largo de la LOPD.

[65] Artículo 20.3 ET.

Según los hechos probados, la empresa coloca en un lugar visible, el escaparate de la tienda, el dispositivo informativo exigido por la LOPD. Por tanto, la trabajadora podía tener conocimiento previo de la existencia del sistema de videovigilancia con fines de control laboral.

En conclusión, en la STC 39/2016 no se establece una vulneración del artículo 18.4 CE, pues, conforme al principio de proporcionalidad, las medidas adoptadas por la empresa a través de la instalación de los dispositivos de videovigilancia han respetado el derecho a la intimidad de carácter personal de la demandante.

La jurisprudencia del TS tiene en cuenta la evolución de la doctrina del TC, como, por ejemplo, a través de la STS (Sala de lo Contencioso-Administrativo, Sección4ª) Sentencia núm. 557/2021 de 26 abril, donde la validez de la aportación de las imágenes captadas a través de los sistemas de videovigilancia no requiere el aviso de forma expresa al trabajador de su posible uso en un proceso sancionador, pues es suficiente con la instalación de los carteles de advertencia al público.

A nivel internacional, cabe destacar que "la posición del TEDH es garantista".[66] Bien es verdad que en la STEDH, de 9 de enero de 2018, en el asunto López Ribalda I, se defendía que la medida tomada por la empresa de instalar dispositivos de videovigilancia donde, a pesar haber instalado los dispositivos informativos en la entrada del lugar de trabajo, no alcanzaba el juicio de proporcionalidad debido a la falta de información de forma concreta a los empleados de la instalación de cámaras ocultas, conforme a lo previsto en la LOPD, y por el carácter discriminatorio de la grabación, pues afectaba a la totalidad de la plantilla durante toda de la jornada y extendiéndose en el tiempo a lo largo de varias semanas.

En contraposición, cabe destacar la STEDH de17 de octubre de 2019, en el asunto López Ribalda II, donde, defendiéndose los mismos fundamentos jurídicos, se concluye que se admite la grabación a través de cámaras ocultas en el lugar de trabajo ante la existencia de sospechas razonables y debidamente acreditadas de irregularidades graves. Por tanto, la superación del test de proporcionalidad radica en las sospechas razonables de las diversas irregularidades que se estaban produciendo.

[66] Monereo Pérez, J. L. y Ortega Lozano, P. L., "Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves." Revista de Jurisprudencia Laboral - Número 8/2019, p. 10.

Por tanto, el problema radica en la "interpretación de cuestiones fácticas objeto de prueba"[67], y no en los fundamentos de derecho. No obstante, cabe destacar que se requiere una argumentación jurídica basada en indicios. Ello implica que la acreditación fehaciente de las sospechas serán necesarias para la admisión de las grabaciones a través de dispositivos de videovigilancia ocultos.

4.2.4 Requisitos

Con el fin de examinar los requisitos del control empresarial, atenderemos a la guía que publicó la AEPD, el 18 de mayo de 2021, con la finalidad de aportar un instrumento práctico de ayuda tanto a las organizaciones públicas como privadas para promover un adecuado cumplimiento de la legislación actual. Además, cabe destacar que la guía se llevó a cabo con la colaboración del Ministerio del Trabajo y Economía Social, de la patronal y diversas organizaciones sindicales.[68]

Los requisitos para el tratamiento de datos personales con fines de vigilancia serán los siguientes.

En primer lugar, los dispositivos de videovigilancia únicamente podrán instalarse cuando no sea posible tomar otra medida que sean menos agresivas para la privacidad e intimidad de los trabajadores. De este modo, la AEPD deja claro el principio de proporcionalidad en la decisión del empleado, donde la relación entre la finalidad que se persigue y el modo de tratamiento de los datos sea la más proporcionada posible. El juicio de proporcionalidad se supera si se cumplen tres requisitos: si la medida adoptada es apta para alcanzar la finalidad (juicio de idoneidad), si no existe otra medida menos lesiva en los derechos del trabajador que tenga la misma eficacia para conseguir el objetivo (juicio de necesidad) y si la medida es equilibrada o ponderada, es decir, si aporta más beneficios para el interés general que desventajas o perjuicios sobre otros valores o derechos en conflicto (juicio de proporcionalidad en sentido estricto).[69]

[67] Monereo Pérez, J. L. y Ortega Lozano, P. L., op. cit., p. 10.
[68] AEPD, "La protección de datos en las relaciones laborales", 2021, p.6.
[69] González González C., "Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016." Revista Aranzadi Doctrinal num. 5/2016 p. 9.

Además, el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29[70] define que los dispositivos de videovigilancia permitirían a la empresa examinar las expresiones faciales de un empleado o descubrir desviaciones en relación con los patrones de movimiento predeterminados. Estas medidas serían un claro ejemplo de falta de proporcionalidad respecto al fin perseguido, pues estarían atentando contra los derechos y libertades de los empleados, y, consecuentemente, estas medidas serían consideradas ilícitas. Además, el tratamiento de datos podría proceder a la creación de perfiles, así como a "la toma de decisiones automatizada"[71]. Por tanto, los dispositivos de videovigilancia no podrán manejarse junto a otros medios tecnológicos, como el reconocimiento facial, pues podría conllevar a medidas totalmente desproporcionadas.

De este modo, la empresa deberá realizar una búsqueda exhaustiva con el fin de encontrar y, posteriormente, adoptar las medidas menos lesivas para los derechos fundamentales de los trabajadores, más expresamente para los derechos de intimidad y protección de datos. La empresa deberá priorizar, por ejemplo, las cámaras que solo habiliten la visualización frente a la grabación de las imágenes, los dispositivos fijos frente a los móviles, los integrados con instalaciones cerradas de televisión frente a los sistemas conectados a la red, etc.[72]

Como podemos observar, la ley no determina un plazo específico para el tratamiento de las imágenes o videos captados por los dispositivos de videovigilancia en el lugar de trabajo, dejándolo así albedrío del empresario y al arbitrio del juez en cada caso. En mi opinión, se deberían regular unos plazos temporales máximos, pues las funciones propias de la dirección y supervisión de la empresa no deberían situarse en un marco temporal tan amplio y ambiguo. Se presume que deberemos acudir al principio de proporcionalidad y prohibición de exceso para analizar la legitimidad en cada caso, pero, en tanto que los trabajadores no someten todo su ser y obrar a la empresa, convendría e interesaría imponer unos límites determinados a la duración de los sistemas de videovigilancia. Asimismo,

[70] El Grupo de Trabajo se estableció conforme al artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo que no depende de la UE en materia de la protección de datos y privacidad.
Sus funciones se encuentran reguladas en el artículo 30 de la Directiva mencionada, así como en el artículo 15 de la Directiva 2002/58/CE.

[71] Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29 (WP 249, 8 de junio de 2017)

[72] Gude Fernández, A., "La videovigilancia laboral y el derecho a la protección de datos de carácter personal", Universidad de Santiago de Compostela, 2014, p. 63. Disponible en https://minerva.usc.es/xmlui/handle/10347/19704 ; Última visita el 10/03/2022.

debemos tener presentes tanto las implicaciones psicológicas como las objeciones éticas que pueden conllevar "una vigilancia permanente en general y de manera especial en los trabajadores".[73]

En segundo lugar, la AEPD define la importancia del principio de minimización conforme con lo previsto en el artículo 5 del RGPD. Ello implica que los datos objeto de tratamiento por parte de la empresa deberán ser "adecuados, pertinentes y limitados"[74] en relación con la finalidad que se persigue.

En el ámbito de los dispositivos de videovigilancia, el principio de minimización implica una reducción en el número de cámaras, pues únicamente se deberán instalar las estrictamente necesarias para cumplir con el control empresarial. Además, la empresa se deberá encargar de analizar los "requisitos técnicos"[75] de las propias cámaras, como por ejemplo el *zoom* seleccionado deberá ser el mínimo posible.

Igualmente, según la AEPD los monitores de grabación deberán ubicarse de manera que solamente puedan acceder a las visualizaciones los responsables de controlar los datos obtenidos a través de los sistemas de videovigilancia. De esta forma, se prohíbe que los clientes o usuarios tengan acceso a las mismas[76].

En tercer y cuarto lugar, en la guía de la AEPD citada a lo largo del presente apartado se señala el deber de información y la limitación territorial en las zonas de descanso y esparcimiento mencionadas anteriormente según la LOPD. Posteriormente, también se determina el deber de implementar las medidas de seguridad que el empresario considere pertinentes en función de los riesgos analizados y, si fuese necesario, la estimación de los impactos que pueda provocar con su decisión[77].

Cabe destacar que si se encargase la gestión a un tercero, será este último el responsable de someter el tratamiento de datos a los requisitos establecidos por la legislación actual.

Por último, respecto a la supresión de los datos, según el artículo 22.3 LOPD, los datos deberán ser eliminados en un plazo máximo de un mes a contar desde su grabación, salvo

[73] Gude Fernández, A., op. cit. p. 49.
[74] AEPD, op. cit., p. 52
[75] AEPD, op. cit., p.52
[76] AEPD, op. cit., p.52
[77] AEPD, op. cit., p.53.

cuando deban ser conservados como prueba de un acto ilícito que atente contra la integridad de las personas, los bienes o las instalaciones. En este caso, las grabaciones serán conferidas a la autoridad que resulte ser competente "en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de su existencia"[78].

4.2.5 Derechos digitales en la negociación colectiva

Los Convenios colectivos también se han pronunciado acerca de la facultad empresarial en relación con los dispositivos de videovigilancia, sin perjuicio de la aplicación del marco legal y los límites inherentes al mismo.

Por ejemplo, en el artículo 37.2 del Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones aprobado en septiembre de 2021, se faculta a las empresas para proceder al tratamiento de las imágenes obtenidas a través de los sistemas de videovigilancia con el objetivo de controlar las obligaciones laborales.[79]

Sin embargo, el citado Convenio colectivo propone el mismo límite territorial que la LOPD en la instalación de los dispositivos de videovigilancia, pues no se admitirán en los lugares destinados al descanso o esparcimiento de los trabajadores.

De esta forma, observamos como los Convenios colectivos se limitan a expresar las limitaciones contenidas en la ley, sin especificar nuevas distinciones que puedan llegar a salvaguardar los derechos e intereses de los trabajadores en mayor medida como, por ejemplo, declarando los supuestos concretos en los que se llevará a cabo esta medida o los plazos determinados en cada caso.

Por otro lado, el artículo 120 del Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, del 29 de diciembre de 2021, también regula el uso de los dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

[78] 22.3 LOPD

[79] Artículo 37.2. Resolución de 3 de septiembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones.

En primer lugar, establece la obligación por parte del empresario de informar previamente de manera "expresa, clara y concisa"[80] a los trabajadores y, en su caso, a sus representantes sobre la existencia de los dispositivos de videovigilancia en el ámbito laboral. Sin embargo, cabe destacar que en el caso de que las cámaras detectasen la comisión flagrante de un acto ilícito por parte de los trabajadores, el deber de informar se presumirá cumplido cuando se hubiese colocado el dispositivo informativo previsto en el artículo 22.4 de la LOPD. De este modo, se puede observar cómo los Convenios colectivos se van adaptando a la ley y a la jurisprudencia, pues esta última previsión se ha visto reflejada tanto en el artículo 89 LOPD como en la STC 39/1016 analizada en el apartado anterior.

Por último, el Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal señala que las empresas podrán hacer uso de los dispositivos de videovigilancia, así como proceder al tratamiento de los datos contenidos en los mismos, siempre y cuando persigan un fin legítimo y respeten los principios de proporcionalidad y mínima intervención. Además, los datos susceptibles de tratamiento "deberán ser adecuados, pertinentes y limitados en relación con los fines para los que son tratados."[81]

4.3 Sistemas de geolocalización

4.3.1 Concepto de geolocalización

La geolocalización se puede definir como "la tecnología que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento"[82].

El uso de los sistemas de geolocalización por parte de las empresas puede llegar a suponer una vulneración del derecho de la intimidad de los trabajadores. Este problema jurídico-laboral ha sido objeto de estudio y preocupación. A nivel nacional, se puede observar a través de las numerosas resoluciones de la AEPD. Por otra parte, a nivel europeo, se puede

[80] Artículo 120. Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal.
[81] Artículo 120. Resolución de 29 de diciembre de 2021, op. cit.
[82] Caletrío, A. B., "Intimidad personal, protección de datos personales y geolocalización", Derecho privado y Constitución, 2015, p. 48

apreciar a través del Dictamen aprobado por el Grupo de Trabajo del artículo 29, el 16 de mayo de 2011, concerniente a los servicios de geolocalización en los teléfonos móviles o a través de las sentencias del TEDH acerca de la vigilancia a través del sistema GPS como, por ejemplo, en el caso Uzún vs Alemania, Secc. 5.ª, de 2 de septiembre de 2010 (asunto 35625/05).

Por tanto, a pesar de las numerosas ventajas que proporcionan los sistemas de geolocalización, en el ámbito laboral puede plantear diversas problemáticas jurídico-laborales en torno al derecho de la intimidad de los trabajadores.

4.3.2 Facultad empresarial de control

En virtud del artículo 90 LOPD, las empresas tienen la facultad para proceder al tratamiento de los datos obtenidos mediante los sistemas de geolocalización con la finalidad de ejercer las funciones propias de control de los trabajadores. Esta facultad viene otorgada a raíz del artículo 20.3 ET que se ha mencionado a lo largo de este trabajo, donde las empresas deberán adoptar las medidas que consideren más oportunas con el fin de supervisar la prestación laboral de sus empleados.

Por otra parte, según el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo del Artículo 29, cabe destacar que el objeto de los dispositivos de geolocalización pueden ser bienes propiedad de la empresa y no la persona trabajadora en sí, como, por ejemplo, los vehículos o los dispositivos móviles.

Por tanto, según el Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29, el tratamiento de los datos recogidos a través de los sistemas de geolocalización se admite si la adopción de la medida va dirigida a controlar el transporte de personas o bienes, favorecer la distribución de recursos o cuando vaya destinada a garantizar la seguridad de los bienes o trabajadores[83]. De este modo, cuando el único deseo de la empresa sea controlar la prestación laboral, deberá estudiarse la posibilidad de adoptar otros medios menos lesivos para los derechos y libertades del trabajador.

[83] Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29 (WP 115, 25 de noviembre de 2005)

Finalmente, el artículo 90.2 LOPD regula el deber de información de la empresa de comunicar de manera "expresa, clara e inequívoca"[84] a sus empleados y, en su caso, a sus representantes, con carácter previo a la instalación de los dispositivos de geolocalización. De esta forma, los trabajadores tendrán conocimiento tanto de la existencia como de su posibilidad para ejercer los derechos de acceso, limitación del tratamiento, rectificación y supresión.

4.3.3 Requisitos

Según la guía que publicó la AEPD, del 18 de mayo de 2021, "los principios de minimización y limitación de la finalidad son plenamente operativos."[85] Ello implica que el empresario únicamente podrá tratar los datos personales que sean estrictamente necesarios para alcanzar la finalidad que se persigue con el fin de evitar recoger datos que sean excesivos o potencialmente ilícitos. Por ejemplo, si el objetivo de la empresa radica en registrar los horarios de los trabajadores, los datos obtenidos a través de los sistemas de geolocalización no deberán ser tratados para comprobar la ubicación del empleado en cada momento, limitándose así a verificar las horas de inicio y terminación de la jornada laboral, conforme a lo previsto en el artículo 34.9 ET acerca del registro diario de la jornada laboral. Por otra parte, la limitación de la finalidad del tratamiento de datos implica que dicha finalidad tiene que encontrarse correctamente "definida y ser comprensible para un usuario medio sin conocimientos jurídicos o técnicos especiales."[86]

En segundo lugar, la AEPD destaca la importancia del principio de proporcionalidad en torno a los sistemas de geolocalización, donde la empresa deberá limitar la adopción de estas medidas a aquellas circunstancias donde no existan otros medios que resulten ser menos invasivos para los derechos y libertades del trabajador.

De esta forma, si bien la doctrina judicial ha admitido la implementación de los sistemas de geolocalización en el ámbito laboral sin necesidad de una negociación previa al amparo del artículo 20.1 ET (Sentencia del Tribunal Superior de Justicia (a partir de ahora, STSJ) Andalucía 1371/2017, STSJ Asturias 3058/2017, STSJ Comunidad Valenciana 1165/2017) siempre y cuando la medida sea informada, el tratamiento de los datos

[84] Artículo 90.2 LOPD
[85] AEPD, op. cit., p.53
[86] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo del Artículo 29 (WP 202, 27 de febrero de 2013)

personales se realice de forma adecuada, y, por último, que la medida adoptada supere un juicio de proporcionalidad.

Sin embargo, son numerosos los casos en los que el juicio de proporcionalidad no se ha superado, como, por ejemplo, en la Sentencia de la Audiencia Nacional (a partir de ahora, SAN) 13/2019, de 6 de febrero, Sala de lo Social, donde la empresa decide implantar un sistema de geolocalización que exigía la aportación del teléfono móvil privado con conexión a internet del trabajador con categoría de repartidor. Esta medida, si bien se encuentra amparada constitucionalmente, según el artículo 38 CE, en el derecho de la libertad de empresa en el ejercicio de su productividad ofreciendo servicios de ubicación que ya ofrecen sus competidores, no llega a superar el juicio de proporcionalidad.

Según la SAN 13/2019 la misma finalidad podría haber sido conseguida a través de otras medidas que suponían una menor intrusión en los derechos de los trabajadores como, por ejemplo, implementar los mismos sistemas de geolocalización en las motocicletas que llevan a cabo los pedidos o en las pulseras con el fin de no exigir una aportación de un bien propio y, sobre todo, sin la recopilación de los datos personales como el número de teléfono móvil o la dirección del correo electrónico a través del cual se obtiene el código para descargarse la aplicación informática por el que se activa el sistema de geolocalización.[87]

Según la AEPD, el riesgo en estos dispositivos radica en el acceso a otra información como, por ejemplo, el comportamiento del conductor al volante, la monitorización o, incluso, la observación constante del trabajador que podría conllevar a un control excesivo por parte del empresario. Por ello, el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29 propone una serie de cautelas. En primer lugar, la previa elaboración de una evaluación del posible impacto de estos sistemas cuando sea la primera vez que la empresa opta por la adopción de estas medidas. En el caso que resultase ser necesaria para llevar a cabo la finalidad especificada y definida, también deberá estudiar su cumplimiento con los principios de proporcionalidad y subsidiariedad.

Por último, cabe destacar que determinadas políticas de las empresas permiten el uso personal de los vehículos profesionales fuera de su jornada de trabajo. En estos casos, la

[87] SAN (Sala de lo Social, Sección 1ª), sentencia núm. 13/2019 de 6 de febrero.

AEPD recomienda optar por la exclusión voluntaria, donde el trabajador podrá desactivar y activar el dispositivo de geolocalización al terminar su jornada laboral.

Por su parte, la jurisprudencia se ha pronunciado acerca del límite temporal de estas medidas. Así, la STSJ Asturias 3058/2017, de 27 de diciembre, Sala de lo Social, establece el deber empresarial de garantizar que estos dispositivos dejen de estar operativos a partir del momento en que termine el horario de trabajo, pues en ese momento "la relación laboral deja de constituir el vínculo entre las partes que ampara al empleador para imponer las medidas implantadas de captación y tratamiento de datos."[88]

4.3.4 Derechos digitales en la negociación colectiva

Los Convenios colectivos no se han mantenido al margen de la regulación de los dispositivos de geolocalización.

En virtud del artículo 37.5 del Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones, del 3 de septiembre de 2021, se faculta a las empresas para tratar los datos personales obtenidos mediante los sistemas de geolocalización con la finalidad de ejercer las funciones de control de la prestación laboral de los trabajadores conforme el marco legal aplicable.

Seguidamente, expone el deber de informar previamente de forma "expresa, clara e inequívoca"[89] acerca de la existencia y características de los dispositivos de geolocalización a los trabajadores y, en su caso, a sus representantes. Además, también se deberá informar acerca de los derechos que pueden ejercer como, por ejemplo los derechos de acceso, limitación del tratamiento, rectificación, y supresión.

Asimismo, el Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, del 29 de diciembre de 2021, también regula el derecho a la intimidad de los trabajadores frente a la utilización de los sistemas de geolocalización en el ámbito laboral. A través de su artículo 121, se exige a los empresarios garantizar

[88] AEPD, op. cit., p. 55

[89] Artículo 37.5. Resolución de 3 de septiembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones.

que estos dispositivos dejen de estar operativos o cesen a partir del momento en que termine la jornada laboral del trabajador.

En resumen, los Convenios colectivos reconocen el derecho de los trabajadores de conocer de manera clara e inequívoca tanto la existencia como las características de los dispositivos de geolocalización. Además, los Convenios colectivos también añaden límites temporales a la regulación actual acerca de la utilización de estos dispositivos, evitando así un uso excesivo e inadecuado por parte del empresario y salvaguardando el derecho a la intimidad de los trabajadores.

4.4 Control biométrico

4.4.1 Concepto de datos biométricos

Según el artículo 4.12 del RGPD, los datos biométricos se podrían definir como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona"[90].

El artículo 9.1 RGPD introduce los datos biométricos en una categoría especial de datos personales, donde queda prohibido su tratamiento, salvo que concurra una de las circunstancias previstas en el artículo 9.2 RGPD como, por ejemplo, en referencia al interés público.

Sin embargo, el artículo 9.1 RGPD únicamente introduce en la categoría especial de datos personales los "datos biométricos dirigidos a identificar de manera unívoca a una persona física"[91], diferenciando así los casos de identificación biométrica de los casos de autentificación o verificación a través del control biométrico.

Esta distinción también ha sido recogida a través del Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del Artículo 29. Por una parte, la identificación biométrica radica en la comparación de los datos biométricos de un sujeto con una serie de plantillas biométricas conservadas en una base de datos. Por otra parte,

[90] Artículo 4.12 del RGPD
[91] Artículo 9.1 RGPD

la autentificación o verificación biométrica se basa en la comparación de los datos biométricos de un sujeto con solo una plantilla biométrica conservada en un único dispositivo.[92]

De este modo, únicamente la identificación biométrica será considerada una categoría especial de protección de datos. Por ello, la AEPD recomienda a las empresas que, en caso de utilizar estos sistemas, opten por una autentificación o verificación biométrica. Además, la AEPD aconseja que el tratamiento de datos biométricos se realice a través de una lectura de los datos almacenados a través de plantillas cifradas en diversos soportes que únicamente puedan ser custodiados por los propios trabajadores, como, por ejemplo, a través de las tarjetas inteligentes.

Un ejemplo de ello sería la utilización de estos sistemas para el fichaje en el lugar de acceso al edificio. En este caso, la AEPD determina que el tratamiento de datos biométricos se realizará por los propios trabajadores a través de la lectura de sus huellas digitales y la consiguiente correspondencia con el número de sus tarjetas. De este modo, el lector se limitará en verificar la correspondencia entre el identificador numérico de la huella del trabajador y su tarjeta.

4.4.2 Facultad empresarial de control

Al igual que en los casos anteriores, en virtud del artículo 20.3 ET, el empresario tendrá la facultar de tomar las medidas que considere más apropiadas con el fin de controlar el cumplimiento de las prestaciones laborales.

Sin embargo, la empresa deberá adoptar sus medidas de control biométrico según la AEPD y en concordancia con las garantías previstas en el RGPD.

En primer lugar, el empresario deberá informar previamente a los trabajadores acerca de la existencia, condiciones y finalidades del tratamiento, prohibiendo así que se utilicen los datos almacenados para otros fines no previstos. De este modo, los datos se deberán suprimir cuando no se relacionen con esa finalidad. Por ejemplo, según el Dictamen 3/2012 sobre evolución de tecnologías biométricas del Grupo de Trabajo del Artículo 29, en el caso de instalar un control biométrico para el acceso a zonas restringidas, los datos

[92] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del Artículo 29 (WP193, 27 de abril de 2012), p. 6

biométricos de aquellos trabajadores que ya no se encuentren autorizados para acceder deberán ser suprimidos.

En segundo lugar, la AEPD define que la instalación deberá realizarse "desde el diseño"[93] por los propios fabricantes de estos sistemas. Ello implicaría, por ejemplo, la supresión inmediata y automática de los datos personales una vez reconocida la plantilla, o el manejo del cifrado para almacenar los datos biométricos.

En tercer lugar, se hace referencia al uso de las plantillas biométricas y los dispositivos personales de lectura con claves cifradas para almacenar los datos, evitando así el acceso a los sujetos no autorizados para ello.

Por último, según la AEPD, en el caso de instalar un sistema de identificación biométrica, la empresa deberá realizar una evaluación de sus posibles impactos.

No obstante, cabe destacar que nos encontramos ante meras recomendaciones de la AEPD, por lo que no hay ninguna previsión específica en el RGPD que imponga límites claros y concisos a las empresas, pudiendo suponer un riesgo para los derechos de los trabajadores si no se articula de forma correcta la reglamentación. Por ello, será fundamental que los convenios colectivos de las empresas acojan tanto las garantías expuestas como otras adicionales con la finalidad que proteger los derechos digitales en el ámbito laboral.

Además, cabe destacar que los convenios colectivos no suelen recoger estas garantías en referencia a los controles biométricos. Así, numerosos convenios colectivos se limitan a establecer el principio de proporcionalidad como condición a la hora de adoptar una medida de control biométrico como el Convenio colectivo para los establecimientos financieros de crédito.

[93] AEPD, op. cit., p. 31

4.5 Teletrabajo

4.5.1 Concepto de teletrabajo

Como consecuencia del confinamiento producido durante la pandemia del COVID-19, los empresarios se vieron en la necesidad de cambiar sus modelos de negocio tradicionales de manera urgente y sin encontrarse programada. Las políticas de teletrabajo fueron unas de las medidas urgentes más destacadas con la finalidad de continuar las prestaciones laborales a distancia.

En este contexto, el Gobierno aprobó el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, que acabó integrándose a nuestro ordenamiento jurídico a través de la Ley 10/2021, de 9 de julio, de trabajo a distancia.

Según el artículo 2 de la Ley 10/2021, de 9 de julio, de trabajo a distancia, el teletrabajo se define como "aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación."[94] De este modo, el teletrabajo se convierte en un nuevo modelo de negocio que forma parte de la digitalización.

4.5.2 Facultad empresarial de control

En virtud del artículo 17 de la Ley 10/2021, de 9 de julio, de trabajo a distancia, nos encontramos con los derechos a la intimidad y a la protección de datos en relación con el uso de los medios telemáticos. En el citado artículo se establece el deber de adecuar el control empresarial a los principios de idoneidad, necesidad y proporcionalidad de las medidas adoptadas conforme a la LOPD.

Además, se prohíbe al empresario exigir la instalación de aplicaciones o programas en los dispositivos digitales que sean propiedad personal del trabajador, ni el uso de los mismos para realizar el trabajo a distancia.

Por último, se establece el deber de la empresa de fijar los criterios que se llevarán a cabo en la utilización de los dispositivos en función de los estándares mínimos fijados en la ley. Para ello, la AEPD publicó diversas recomendaciones con la finalidad de adecuar las

[94] Artículo 2 de la Ley 10/2021, de 9 de julio, de trabajo a distancia

nuevas políticas de teletrabajo al RGPD. De este modo, las medidas adoptadas por la empresa a través de las políticas del teletrabajo deberán determinarse tras haber realizado una evaluación de riesgos, analizando así la proporcionalidad entre las ventajas del acceso a distancia y el riesgo potencial que sufre el acceso a los datos de carácter personal.

5. CONCLUSIONES

A continuación, exponemos las conclusiones alcanzadas a lo largo del presente trabajo de investigación:

I. El derecho a la protección de datos es un derecho fundamental autónomo e independiente del derecho a la intimidad que reconoce a todos los sujetos la facultad de disponer y controlar sus datos personales, situando así el consentimiento y el derecho de información en el eje central del ejercicio de este derecho.

II. Según el artículo 20.3 ET, no se requiere el consentimiento de los trabajadores cuando el empresario adopte las medidas que considere oportunas para controlar y supervisar el cumplimiento de las prestaciones laborales.

III. Los dispositivos digitales que el empresario pone a disposición de sus empleados se encuentran dentro de la esfera de la propiedad del empresario, adquiriendo así la facultad para controlar el uso de los mismos, siempre que cumpla con el deber de informar a sus trabajadores y los límites previstos en la ley.

IV. Cabe destacar el vacío legal en la regulación del *bring your own device* o "trae tu propio dispositivo". En el presente trabajo de fin de grado se llega a la conclusión que los dispositivos aportados por los empleados para trabajar se dividirán en dos perfiles: uno personal amparado bajo el artículo 18 ET donde se regula la inviolabilidad de la persona del trabajador y otro perfil profesional amparado por el artículo 20.3 ET donde el empresario podrá ejercer cierto control, pues la empresa será la encargada de garantizar el cumplimiento de la normativa de la protección de datos.

V. Respecto de los sistemas de videovigilancia, el deber de información radica en la colocación de un dispositivo informativo en los lugares videovigilados de tal forma que sean suficientemente visibles. La modificación del deber de información previamente indicado se produjo a raíz de la STC 39/1016, de 3 de marzo, pues, con anterioridad se requería informar de forma directa a los trabajadores.

VI. A la hora de valorar la licitud del control empresarial, la doctrina jurisprudencial analizará las medidas en función el principio de proporcionalidad a través de los cuatro factores siguientes: idoneidad, necesidad, justificación y ponderación.

VII. La jurisprudencia del TDEH realiza su análisis del juicio de proporcionalidad a través de los siguientes cinco factores: el grado de intrusión de la empresa, la existencia de una razón justificada y legítima acerca de la medida adoptada por la empresa, la existencia o no de otros medios que resulten menos intrusivos para alcanzar el mismo fin, el destino perseguido por la empresa y las garantías previstas para el empleado

VIII. En virtud del artículo 5.1 del RGPD se consagran los límites de la facultad empresarial en torno a los dispositivos digitales a través de los principios de licitud, lealtad, transparencia, limitación de la finalidad del tratamiento, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad, y, finalmente, el principio de proporcionalidad.

IX. Cabe destacar que la ley no especifica un plazo determinado para el tratamiento de los datos personales de los trabajadores en ninguno de los dispositivos digitales o de geolocalización, exponiendo así a los trabajadores una pluralidad de supuestos que atentan directamente contra sus derechos personales. En mi opinión, sería preciso que el legislador incorporase en la ley unos plazos temporales máximos, pues las funciones propias del control y supervisión del empresario no deberían situarse en un marco temporal tan amplio y ambiguo.

Por el contrario, en los dispositivos de videovigilancia el legislador sí incorpora un límite temporal a través del artículo 22.3 LOPD, donde los datos deberán ser eliminados en un plazo máximo de un mes a contar desde su grabación.

X. Parte de la doctrina denuncia las limitaciones que presenta la ley en esta materia ante la continua evolución de la tecnología y el riesgo de que la normativa actual resulte obsoleta. Por ello, ante la falta de actuación por parte del legislador, la jurisprudencia, las recomendaciones de la AEPD y los convenios colectivos resultan cruciales a la hora de adaptarse y completar la ley para hacer frente a los nuevos casos que con certeza irán apareciendo en un futuro.

XI. Por último, cabe destacar la insuficiencia claridad del RGPD al agrupar a todos los dispositivos digitales en un conjunto sin diferenciar las características y procedimientos teniendo en cuenta las particularidades de cada uno de ellos.

6. BIBLIOGRAFÍA

6.1 Legislación

6.1.1 Comunitario

Europea, U. (2021). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo del Artículo 29 (WP 202, 27 de febrero de 2013)

Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29 (WP 115, 25 de noviembre de 2005)

Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29 (WP 249, 8 de junio de 2017)

Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del Artículo 29 (WP193, 27 de abril de 2012)

6.1.2 Nacional

Agencia Española de Protección de Datos. La protección de datos en las relaciones laborales (2021)

Agencia Española de Protección de Datos. Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (2020)

Agencia Española de Protección de Datos. Guía sobre el uso de videocámaras para seguridad y otras finalidades (2021)

Constitución española (BOE núm.311, de 29 de diciembre de 1978).

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. («BOE» núm. 296, de 12 de diciembre de 2006)

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. («BOE» núm. 115, de 14 de mayo de 1982).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales («BOE» núm. 294, de 6 de diciembre de 2018).

Ley 10/2021, de 9 de julio, de trabajo a distancia. («BOE» núm. 164, de 10 de julio de 2021)

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 («BOE» núm. 255, de 24 de octubre de 2015).

Resolución de 11 de junio de 2020, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Teleinformática y Comunicaciones, SAU («BOE» núm. 173, de 22 de junio de 2020)

Resolución de 23 de diciembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Telefónica Ingeniería de Seguridad SAU. («BOE» núm. 6, de 7 de enero de 2020)

Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal. («BOE» núm. 10, de 12 de enero de 2022)

Resolución de 3 de septiembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal de empresas de servicios auxiliares de información, recepción, control de accesos y comprobación de instalaciones. («BOE» núm. 223, de 17 de septiembre de 2021)

Resolución de 5 de octubre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo para los establecimientos financieros de crédito. («BOE» núm. 247, de 15 de octubre de 2021)

6.2 Jurisprudencia

6.2.1 Jurisprudencia nacional

SAN Madrid (Sala de lo Social, Sección 1ª), sentencia núm. 13/2019 de 6 de febrero. Disponible en https://www.poderjudicial.es/search/AN/openDocument/8ed60e51766c4e3e/20190219 ; última consulta el 1/04/2022

Sentencia del Juzgado de lo Social núm. 2 de Madrid, sentencia núm. 93/2019 de 12 febrero. Disponible en https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad82d9b0000018136f0c8d697e94a00&marginal=AS\2020\837&docguid=I81d6dde0601a11eaba38bc5e74f2b459&ds=ARZ_LEGIS_CS&infotype=arz_juris;&spos=2&epos=2&td=0&predefinedRelationshipsType=documentRetrieval&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName= ; última consulta el 24/05/2022).

STC 170/2013, de 7 de octubre de 2013 (Recurso de amparo 2907-2011). (BOE núm. 267, de 7 de noviembre de 2013). Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-11681 ; última consulta el 5/03/2022.

STC 196/2004, de 15 de noviembre (BOE núm. 306, de 21 de diciembre de 2004). Disponible en http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/5201; última consulta el 2/03/2022).

STC 241/2012, de 17 de diciembre (BOE núm. 19, de 22 de enero de 2013). Disponible en http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/23200 ; última consulta el 6/03/2022.

STC 254/1993, de 20 de julio (BOE núm. 197, de 18 de agosto de 1993). Disponible en http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383 ; última consulta el 2/03/2022.

STC 292/2000, de 30 de noviembre (BOE núm. 4, de 04 de enero de 2001). Disponible en http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276. ; última consulta el 2/03/2022.

STC 39/2016, de 3 de marzo (BOE núm. 85, de 08 de abril de 2016). Disponible en https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/24843 ; última consulta el 18/03/2022.

STS (Sala de lo Contencioso-Administrativo, Sección4ª) Sentencia núm. 557/2021 de 26 abril. RJ 2021\1927. Disponible en https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad6adc50000018117f8c9bd49886348&marginal=RJ\2021\1927&docguid=Ic512d3b0b2cc11eb86f8c892fef48f92&ds=ARZ_LEGIS_CS&infotype=arz_juris;&spos=1&epos=1&td=499&predefinedRelationshipsType=documentRetrieval&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName= ; última consulta el 20/05/2022.

STS núm. 489/2018, de 23 de octubre. Disponible en https://www.poderjudicial.es/search/indexAN.jsp# ; última consulta el 31/05/2022.

STS núm. 528/2014, de 16 de junio. Disponible en https://www.poderjudicial.es/search/indexAN.jsp# ; última consulta el 31/05/2022.

STSJ Andalucía, Málaga (Sala de lo Social, Sección1ª), sentencia núm. 1371/2017 de 19 julio. Disponible en https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad82d9a000001804823f90a05f0cdcf&marginal=AS\2017\1847&docguid=Ie6ad74e0aa3711e79efd010000000000&ds=ARZ_LEGIS_CS&infotype=arz_juris;&spos=2&epos=2&td=144&predefinedRelationshipsType=documentRetrieval&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName= ; última consulta el 1/04/2022

STSJ Asturias (Sala de lo Social, Sección1ª), sentencia núm. 3058/2017, de 27 de diciembre. Disponible en https://www.poderjudicial.es/search/AN/openDocument/a5ea139c2252ec9a/20180208 ; última consulta el 4/04/2022

STSJ Castilla-La Mancha, (Sala de lo Social, Sección2ª) Sentencia núm. 515/2021 de 25 marzo. Disponible en

https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad6adc50000018117b5a87e52e93888&marginal=AS\2021\1241&docguid=Ie4612730bf6011eb8ad99e12f2e2528f&ds=ARZ_LEGIS_CS&infotype=arz_juris;&spos=1&epos=1&td=6&predefinedRelationshipsType=documentRetrieval&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName= ; última consulta el 20/05/2022

STSJ Comunidad Valenciana (Sala de lo Social, Sección1ª), sentencia núm. 1165/2017 de 2 mayo. Disponible en https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad82d9b00000180482e546ce51c6f7f&marginal=JUR\2017\221347&docguid=Iaa99cb00943611e797590100000000000&ds=ARZ_LEGIS_CS&infotype=arz_juris;&spos=1&epos=1&td=49&predefinedRelationshipsType=documentRetrieval&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName= ; última consulta el 1/04/2022

6.2.2 Jurisprudencia comunitaria

STEDH de 3 de abril de 2007, asunto Copland contra Reino Unido, núm. 62617/00. Disponible en https://www.mjusticia.gob.es/es/AreaInternacional/TribunalEuropeo/Documents/1292429139374-Trad._Sentencia_COPLAND_c.REINO_UNIDO.pdf ; última consulta el 6/03/2022.

STEDH de17 de octubre de 2019, asunto López Ribalda y otros contra España, Demandas nº 1874/13 y 8567/13. Disponible en https://www.mjusticia.gob.es/es/AreaInternacional/TribunalEuropeo/Documents/Sentencia%20L%C3%B3pez%20Ribalda%20c.%20Espa%C3%B1a.pdf ; última consulta el 26/03/2022

6. 3 Obras doctrinales y recursos de internet

Andrés Ricart G. “Recomendaciones para el teletrabajo”, *Thomson Reuters*, 24 de junio de 2020. Disponible en https://www.legaltoday.com/colaborador/andres-ricart/ ; última consulta el 24/05/2022.

Arrivasplata Reyes, F. D., “Monitorización de la navegación en internet en el «BYOD»: exigencias del empleador en el marco de la ley de protección de datos personales”, *SPDTSS,* 2021. Disponible en

https://www.spdtss.org.pe/articulos_congreso/monitorizacion-de-la-navegacion-en-internet-en-el-byod-exigencias-del-empleador-en-el-marco-de-la-ley-de-proteccion-de-datos-personales/ ; última consulta el 23/05/2022)

Ballesteros, I. J. C., "Videovigilancia laboral y derecho fundamental a la protección de datos". *Temas laborales: Revista andaluza de trabajo y bienestar social*, n. 136, 2017, pp. 129-156.

Caletrío, A. B., "Intimidad personal, protección de datos personales y geolocalización". *Derecho privado y Constitución*, n. 29, 2015, pp. 47-82.

Deloitte, "Reescribiendo las reglas para la era de digital. Tendencias Globales en Capital Humano 2017", *Deloitte University Press*, 2017, Disponible en https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/human-capital/2017_Global-Tendencias-Capital-Humano.pdf ; última consulta el 26/03/2022.

Elizalde Purroy I. "España | ¿Posible delito por acceso al ordenador y al correo electrónico del trabajador/a?", *Cuatrecasas*, 1 de junio de 2021. Disponible en https://www.cuatrecasas.com/es/spain/articulo/puede-constituir-delito-acceso-ordenador-correo-electronico-persona-trabajadora ; última consulta el 31/05/2022.

Espuga Torné, G., "La actual situación de emergencia sanitaria causada por la pandemia global de la COVID-19 ha provocado un cambio de paradigma en la organización y realización del trabajo. Este cambio de modelo, basado en el teletrabajo, al que han llegado mejor preparadas las empresas con un alto grado de digitalización, está llamado a permanecer una vez superada la pandemia", *Thomson Reuters*, 24 de junio de 2020. Disponible en https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/teletrabajo-y-derecho-a-la-desconexion-digital-en-al-ambito-laboral-en-tiempos-de-covid-19-2020-06-24/ ; última consulta el 22/05/2022.

González González C., "Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016." *Revista Aranzadi Doctrinal* num. 5/2016 p. 9.

Grupo Atico34, "El fenómeno BYOD y la protección de datos", *Grupo Atico34*, 2020. Disponible en https://protecciondatos-

lopd.com/empresas/byod/#:~:text=BYOD%2C%20siglas%20en%20ingl%C3%A9s%20para,de%20datos%20y%20la%20ciberseguridad ; última consulta el 22/05/2022.

Gude Fernández, A., "La videovigilancia laboral y el derecho a la protección de datos de carácter personal". *Universidad de Santiago de Compostela*, 2014, Disponible en https://minerva.usc.es/xmlui/handle/10347/19704 ; Última visita el 10/03/2022.

Monereo Pérez, J. L. y Ortega Lozano, P. L., "Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves." *Revista de Jurisprudencia Laboral*, n. 8/2019, 2019.

Pérez de los Cobos Orihuel F. y García Rubio M. A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Revista Española de Derecho del Trabajo*, n. 196/2017, 2017.

Pérez Luño A. E., "Manual de informática y derecho", *Barcelona: Ariel*, 1996, p. 43.

Quílez Moreno J. M., "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*, n. 217/2019, 2019.

Sánchez-Ostiz, J. C., & Sancha, J. F., "Novedades en el ámbito laboral de la nueva Ley Orgánica de Protección de Datos". *Actualidad Jurídica Aranzadi*, n. 947, 2018.

Sanllehí, A., & Ramón, J., "Prevención del delito en la empresa: límites ético–jurídicos en la implementación de sistemas de videovigilancia". *Revista Electrónica de Ciencia Penal y Criminología*, 2009.

Sempere Navarro, A.V. y San Martín Mazzucconi, C., "Nuevas tecnologías y relaciones laborales: el estado de la cuestión", *Revista de Derecho* vol. 11, 2010, pp. 260-262 y 285-286.

Slotnisky, D., "Transformación digital: cómo las empresas y los profesionales deben adaptarse a esta revolución". *Digital House. Coding School*, 2016.

Spremolla, G. C., “El trabajo en la era digital”, *Revista de derecho*, *16*(31), 2016, pp. 103-123.

Tortosa Miralles, J. A., “El uso del correo electrónico en el trabajo”. *Universitat Jaume I*, 2016. Disponible en http://repositori.uji.es/xmlui/handle/10234/164466 ; última consulta el 5/03/2022.

6.4 Otros recursos

Real Academia Española. Disponible en https://dle.rae.es/ ; última consulta el 5/03/2022.