FACULTAD DE DERECHO

PRIVACIDAD, INTIMIDAD Y PROTECCIÓN DE DATOS EN LA RELACIÓN LABORAL

Autor: Carmen Pérez Gómez

5º E3 - C

Derecho Laboral

Tutor: Dolores Carrillo Márquez

Madrid

Abril 2022

RESUMEN

La presente investigación trata de dar una visión general de la importancia del derecho a la privacidad, el derecho a la intimidad y el derecho a la protección de datos en el contexto de las relaciones laborales. En primer lugar, se ha concluido que no existe delimitación conceptual de los derechos mencionados. Por este motivo, se procederá a una definición exhaustiva y motivada de cada uno de ellos. Asimismo, con el fin de aportar una mayor comprensión al estudio del trabajo completo, se comenzará la exposición con la enumeración de los principios constitucionales básicos concernientes a la materia. De esta manera, resultará más sencillo comprender los litigios laborales que se mencionen. Análogamente, cabe apuntar que las nuevas tecnologías pueden generar riesgos para el trabajador. Es por ello por lo que ha resultado interesante estudiar tanto los mecanismos de control empresarial más relevantes (ordenador, correo electrónico, historial de navegación y videovigilancia) como sus límites. De esta manera, se realizará un repaso por la normativa, jurisprudencia y doctrina española. Asimismo, se hará mención expresa a los pronunciamientos jurisprudenciales más relevantes de los tribunales europeos. De igual modo, se abordarán los retos empresariales ocasionados por la incidencia sanitaria generada por la enfermedad Covid-19. Finalmente, se tendrán en cuenta los requisitos necesarios para evitar la vulneración de los derechos fundamentales a la privacidad, intimidad y protección de datos durante la acreditación de prueba en un proceso judicial.

PALABRAS CLAVE

- Derecho a la privacidad
- Derecho a la intimidad
- Derecho a la protección de datos
- Nuevas tecnologías
- Poder empresarial
- Mecanismos de control
- Informe pericial

ABSTRACT

This research attempts to give an overview of the importance of the right to privacy, the right to intimacy and the right to data protection in the context of labor relations. First of all, it has been concluded that there is no conceptual delimitation of the aforementioned rights. For this reason, we will proceed to an exhaustive and reasoned definition of each of them. Likewise, in order to provide a better understanding of the study of the entire work, the exposition will begin with the enumeration of the basic constitutional principles concerning the matter. In this way, it will be easier to understand the labor litigation mentioned. Similarly, it should be noted that new technologies can generate risks for the worker. For this reason, it has been interesting to study both the most relevant corporate control mechanisms (computer, e-mail, browsing history and video surveillance) and their limits. In this way, a review will be made of Spanish regulations, case law and doctrine. Likewise, express mention will be made of the most relevant jurisprudential pronouncements of the European courts. Likewise, the business challenges caused by the health incidence generated by the Covid-19 disease will be addressed. Finally, the necessary requirements to avoid the violation of the fundamental rights to privacy, intimacy and data protection during the accreditation of evidence in a judicial process will be taken into account.

KEY WORDS

- Right to privacy
- Right to data protection
- New technologies
- Corporate power
- Control mechanisms
- Expert report

ÍNDICE

LISTADO DE ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
Art.	Artículo
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CEPD	Comité Europeo de Protección de Datos
DPO	Delegado de Protección de Datos
ET	Estatuto de los Trabajadores
JS	Juzgado de lo Social
L	Ley
LEC	Ley de Enjuiciamiento Civil
LO	Ley Orgánica
LOAES	Ley Orgánica de los Estados de Alarma, Excepción y Sitio
LOPD	Ley Orgánica de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
LOPJ	Ley Orgánica del Poder Judicial
LPRL	Ley de Prevención de Riesgos Laborales
LRJS	Ley Reguladora de la Jurisdicción Social
RD	Real Decreto
Rec.	Recurso
RGPD	Reglamento General de Protección de Datos
S	Sentencia

TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
UE	Unión Europea

1. INTRODUCCIÓN

Hoy día, podemos afirmar que nos encontramos en el contexto de una cuarta revolución industrial basada en el predominio de la realidad digital. Esta revolución también denominada "industria 4.0" está alterando las reglas del juego en lo referente a la producción, mano de obra, operaciones empresariales y relaciones laborales (Cotteleer y Snideran, 2018).

En primer lugar, cabe apuntar que un buen uso de lo digital ayudará a las organizaciones a crecer y aprovechar las oportunidades emergentes. No obstante, se ha de advertir que la tecnología en ocasiones se traduce en riesgos para el trabajador.

Este último punto es la pieza clave objeto de estudio en el presente trabajo pues, mediante la digitalización, las empresas tienen la capacidad de recopilar extensos informes de datos de sus trabajadores, lo que puede en ocasiones comportar la vulneración de sus derechos fundamentales (Martínez, 2021). En el mismo sentido, las personas son cada vez más celosas de su esfera privada en todos los ámbitos de la vida (el terreno de la salud, la familia o el laboral, por ejemplo).

Entre los derechos que pueden verse afectados, sobresalen: el derecho a la intimidad, derecho a la privacidad y derecho a la protección de datos. Durante la búsqueda de información para la presente investigación se ha llegado a la conclusión de que, a lo largo de la historia, los tres conceptos expuestos han sido utilizados de manera indistinta. No obstante, cada uno de ellos es merecedor de su propia delimitación, por lo que en el segundo apartado analizaremos qué aspectos de la vida de una persona ampara cada derecho, y concretamente desde la perspectiva de las relaciones laborales.

En lo referente a los derechos de los trabajadores, es preciso detenerse en "los derechos inespecíficos" pues pese a que no exista un tratamiento articulado de los mismos, su estudio es interesante (Crespo, 2018). Se trata de derechos fundamentales que toda persona posee en cualquier ámbito de su vida, incluido el laboral (Orrico, 2019)[1]. Es decir, un contrato de trabajo no puede suponer la privación de derechos que la constitución reconoce a un ciudadano y cuya protección ante posibles lesiones está

[1] En el mismo sentido la autora defiende que *"son derechos que, no teniendo un contenido exclusivamente laboral, tienen importantes repercusiones en el ámbito laboral, en tanto que el trabajador los ostenta por su condición de ciudadano y, por ende, los disfruta también en el ámbito de las relaciones laborales",* y Manuel Carlos Palomeque López quien adivierte que *"se convierten en verdaderos derechos laborales por razón de sujeto y de la naturaleza de la relación jurídicas en que se hacen valer, en derechos constitucionales laborales inespecíficos".*

garantizada (STC 88/1985)[2]. No obstante, pese a que los derechos no desaparecen, sí pueden verse limitados (que no dañados) cuando exista y esté justificado el interés o la necesidad empresarial (Orrico, 2019).

Habida cuenta lo expuesto, es una realidad que ha habido numerosos pleitos en materia de protección de datos, intimidad y privacidad en el seno de las relaciones laborales ya que, no existe pauta exacta que resuelva estos casos, sino que se ha de atender a una ponderación de los derechos en juego (Orrico, 2019). En el mismo sentido se pronuncian otros autores advirtiendo sobre la "*patente necesidad de recurrir al mecanismo de ponderación de bienes"* en este contexto (Martínez de Pisón, 2016).

Consecuentemente, a lo largo de los últimos años y, con el objetivo de luchar contra el abuso de la trata ilícita de datos tanto en el seno de las relaciones laborales como en el resto de los ámbitos de la vida de una persona, el marco jurídico español se ha enfrentado a la necesidad de actualizar sus leyes para amparar los datos personales de Internet[3].

La normativa española aplicable en este contexto es: la Constitución Española, El Reglamento General de Protección de datos (2016/679) y sus respectivas correcciones de 2018 y 2021, La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (3/2018) y el Real Decreto por el que se aprueba el estatuto de la Agencia Española de Protección de Datos (389/2021).

Si bien es cierto, muchas veces no resultan suficiente por lo que la la jurisprudencia y la doctrina han tenido un papel fundamental como guía para los tribunales en casos en los que concurra conflicto concerniente a la materia (Orrico, 2019).

1.1 Justificación

El derecho a la privacidad, intimidad y protección de datos es una cuestión a la orden del día en el seno de las relaciones laborales, es por ello por lo que se ha seleccionado este tema como objeto de investigación.

En los últimos años han sido diversas las sentencias relacionadas con la materia pues en el ámbito de la trata de datos en la relación laboral, la línea de lo que está

[2] Tribunal Constitucional (Pleno). Sentencia núm. 88/1985, de 19 de julio de 1985. ECLI:ES:TC:1985:88

[3] Véase: en 2018 la nueva LOPDDG sustituye a la antigua LOPD e incluye en su objeto la protección de derechos digitales. *"En este sentido, incorpora puntos muy a tener en cuenta, como el derecho al olvido o a la portabilidad, además de cambios en la obtención del consentimiento para recoger y usar la información personal*" (Grupo Atico34, 2018).

permitido y lo que no, no se encuentra siempre bien definida y es precisamente esta difusión la que hace que colisionen derechos de ambas partes.

Adicionalmente, la llegada de la pandemia en 2020 cambió el escenario laboral y advirtió sobre la importancia de las empresas de mantenerse actualizadas para así respetar los derechos de los trabajadores que componen las plantillas. Este aspecto ha sido otro de los motivos por los que ha resultado interesante profundizar en la materia. De esta manera, se investigará sobre el poder del empresario en el contexto de una situación protagonizada por la incertidumbre y los cambios normativos. Habida cuenta de lo expuesto, se examinará cómo se relacionan el derecho a la salud pública con los derechos de los trabajadores.

Sin lugar a duda, se trata de algo que hoy continúa generando inseguridad jurídica para los trabajadores de las empresas que, bien no han sabido implementar las medidas oportunas y han llegado tarde a respetar la legalidad de los datos de sus trabajadores, bien han decidido quebrantar intencionadamente toda norma por considerar que no se ajustaba a las actuaciones que venían ejecutando.

Así mismo, otro de los motivos que han llevado al estudio de esta investigación ha sido la llegada del "Metaverso"[4] y sus posibles "ciberriesgos". Hoy día, los expertos se enfrentan a uno de los mayores retos de la materia pues están confeccionando las normas y los principios que regulen esta nueva realidad ya que los agentes que participen en él "*no escapan a la normativa de los países en los que operen*" (Esteban, 2022).

En resumen, el Derecho Laboral es un derecho muy vivo, que se encuentra en constante evolución y adaptándose día a día a las exigencias sociales. Por este motivo y los expuestos anteriormente, considero que el tema de esta investigación resulta interesante y provechoso no solo para los expertos en la materia sino también para empleadores y empleados que desconozcan tanto las líneas rojas que no se han de traspasar como los principios a respetar pues, insistimos que se trata de derechos que en la actualidad están en primera plana.

[4] El Metaverso puede definirse como *"una combinación de lo físico y lo digital representando la idea de que los usuarios serán capaces de interactuar y realizar transacciones en mundos totalmente digitales"* (de Mendizabal, 2022).

1.2 Objetivos y metodología

El presente trabajo tiene como objetivo principal el estudio en profundidad de los derechos a la privacidad, intimidad y relación de datos en el seno de las relaciones laborales. Para ello investigaremos:

- Cuáles son las diferencias entre "privacidad", "intimidad" y "protección de datos". Como se ha afirmado anteriormente, hoy día el ordenamiento jurídico español no cuenta con definiciones claras sobre tales expresiones, por lo que se busca profundizar en lo establecido por la jurisprudencia y la doctrina para, de esta manera, delimitarlos.

- Conocer los principios constitucionales referentes a la intimidad y privacidad, así como los principios básicos en materia de protección de datos. Su comprensión resulta esencial tanto para la persona encargada de la trata de datos como para el propio afectado. Para ello, se seguirá lo establecido en la CE, los pronunciamientos judiciales, la doctrina y la Agencia Española de Protección de Datos (en adelante, "AEPD") fundamentalmente.

- Por otro lado, se estudiarán los principales mecanismos de control laboral, es decir, los medios más habituales a través de los cuales el empleador recoge información del trabajador: el ordenador del trabajador, correo electrónico, historial de navegación y las cámaras de videovigilancia. Pese a que estas cuestiones puedan resultar perfectamente desglosables en numerosos estudios individuales, se realizará una visión global para entender la materia de manera conjunta y no tanto por medio de secciones separadas. Para ello, se seguirá lo establecido en la normativa, jurisprudencia y doctrina laboralista. Análogamente, se estudiarán casos reales que fueron notablemente influyentes para las empresas y su régimen de protección de datos entre los que cabe destacar: *el Caso Bârbulescu II, el Caso Inditex y el Caso López Ribalda II*.

- Como se ha anticipado, en la presente investigación se busca detallar los poderes del empresario en el contexto de la pandemia. Es necesario no eludir las consecuencias que la pandemia de la Covid-19 ha ocasionado y poner especial atención en las actuaciones de los empresarios en estos momentos. En este punto,

se hará especial mención a lo establecido por la AEPD. Las dudas o problemas más frecuentes que se pretenden resolver son: la legalidad de la toma de temperatura a los trabajadores, la geolocalización de estos, la necesidad de consentimiento del empleado para la trata de datos en casos de fuerza mayor o los medios utilizados para ello.

Para el desarrollo de este apartado, se ha empleado una metodología diferente al resto de la investigación. Se tratará de un modelo basado en la estructura "pregunta-respuesta" pues se ha considerado que, debido a la gran batería de cuestiones sobre la materia, es un método dinámico que ayuda mejor al lector a comprender su contenido.

- Por último, desde una perspectiva adjetiva, se pretende estudiar la necesidad de los informes periciales para la validez de las pruebas en los casos en los que entren en juego derechos de la esfera privada de la persona. De esta manera se expone la importancia de los derechos a la privacidad, intimidad y protección de datos en sede judicial.

  Es posible que el lector se sorprenda al encontrarse con el apartado sexto de la presente investigación, no obstante, he considerado importante no olvidar las posibles vulneraciones en sede judicial de los derechos fundamentales estudiados por vía de acreditación de prueba.

Las fuentes utilizadas cambian en función del contenido. Si bien es cierto, en todo apartado se seguirá únicamente de lo dispuesto en la norma, la jurisprudencia y la variada doctrina relacionada con la materia.

Gracias a la información que me aportaron las distintas fuentes, pude tener una visión mucho más real y esclarecedora de lo que suponen la privacidad, intimidad y protección de datos en el seno de las relaciones laborales.

Finalmente, con la información recopilada, y un conocimiento profundo en la materia, pude elaborar el presente trabajo y así cumplir con los objetivos del mismo.

2. DELIMITACIÓN CONCEPTUAL

Con el objetivo de establecer un orden en lo referente a la estructura de esta investigación, se ha de comenzar por la delimitación conceptual de los derechos a la privacidad, la protección de datos y la intimidad. De esta manera, resultará más sencillo comprender el resto del contenido por abordar.

En primer lugar, es preciso recordar que estos derechos se posicionan en una situación de riesgo resultado de la globalización, que trae consigo habituales menoscabos en la esfera privada de la persona.

No obstante, pese a que los tres términos mencionados versan sobre particularidades semejantes, cada uno de ellos conserva una definición individualizada y no inalterable, más bien sujeta a la realidad de cada momento.

Durante la búsqueda de información para la presente investigación, se ha llegado a la conclusión de que a lo largo de la historia se han utilizado indistintamente los tres derechos para referirse a lo mismo. Por consiguiente, la sociedad se topa con una innegable inseguridad y con la necesidad de conceptualización pues, ante posibles intromisiones en la esfera privada, se ha de tener posibilidad de conocimiento sobre el derecho se puede ver afectado.

Habida cuenta lo anterior, el presente apartado tiene por objeto establecer las diferencias oportunas y evitar la vacilación entre conceptos, mediante el estudio de la norma, la jurisprudencia, y la doctrina constitucional y laboral.

2.1 Diferencias entre intimidad, privacidad y protección de datos

- Privacidad

Al ser el término "privacidad" un concepto tan amplio, hoy día resulta complejo establecer una delimitación exhaustiva del mismo.

Pese a existir mucha literatura en relación con la materia, *"no contamos con una explicación adecuada del sentido y valor de la privacidad"* (Toscano, 2017). Como se ha adelantado, se ha ido equiparando este concepto tanto al derecho a la intimidad como al derecho a la protección de datos y por ello se habla de "*caos de la privacidad*" (Toscano, 2017).

En el mismo sentido, Thomson (citado en Toscano, 2017) plantea en su investigación que *"quizá la cosa más sorprendente acerca del derecho a la privacidad es que nadie parece tener una idea muy clara de lo que es".*

Por lo anterior, la Gran Sala del TEDH ha reparado en la necesidad de definir con claridad el concepto y ha expuesto lo siguiente: *"el Tribunal recuerda que el concepto de "privacidad" es un concepto amplio, que no se presta a una definición exhaustiva. Ampara la integridad física y moral de una persona, así como múltiples aspectos de la identidad física y social de una persona. Incluye los elementos de identificación de una persona, tales como su nombre o fotografía", "el concepto de privacidad no se limita a un "círculo íntimo" donde cada uno puede disponer de su vida personal sin intervención externa, sino que también engloba el derecho a llevar una "vida privada social", es decir, la posibilidad de que una persona se vincule y desarrolle relaciones con sus semejantes y con el mundo exterior. En este sentido, no excluye las actividades profesionales, ni las actividades que se desarrollan en un lugar público. De hecho, existe una zona de interacción entre el individuo y los demás que, incluso en un contexto público, puede pertenecer a la vida privada"* (STEDH JUR\2019\289974)[5].

Habida cuenta lo anterior, se puede concluir que lo más confuso es establecer una diferencia entre el derecho a la intimidad y la privacidad en todos sus extremos. Además, la complejidad aumenta si se comparan los términos con los propios del derecho anglófono, italiano o francés, pues lo que allí significa "derecho a la privacidad" en España se trata de todo lo concerniente al derecho a la intimidad (Toscano, 2017).

Según Castilla (citado en Toscano, 2017) el primer paso para distinguir estos conceptos es atender a los tipos de actuaciones de una persona que, según su palabra son "*públicas, privadas e íntimas*". Pese a que lo complejo reside en analizar los dos últimos términos, cabe apuntar que, si se definen individualmente los tres, será más sencillo diferenciarlos.

En primer lugar, Castilla considera públicas las acciones de una persona que se llevan a cabo a la vista de terceros. Por otro lado, son privadas aquellas acciones que, pudiendo ser públicas, el individuo delibera y decide que tendrán lugar en un espacio privado y, por tanto, fuera del alcance de terceros. Son estas deliberaciones las que hacen

[5] Tribunal Europeo de Derechos Humanos. Sentencia de 17 de octubre de 2019. Caso López Ribalda II contra España. ECLI:CE:ECHR:2019:1017JUD000187413

que algo se convierta en privado, pero no necesariamente tienen porque ser íntimas. Por último, serán intimas aquellas actuaciones a priori imperceptibles e inobservables por terceros, pertenecientes a lo interno de una persona y que solo se puede llegar a ellas por medio de las palabras o actitudes del individuo (Castilla citado en Toscano, 2017).

En el mismo sentido se han pronunciado autores planteado que *"la privacidad es aquel espacio que una persona legítimamente quiere mantener alejado del conocimiento del resto"* (Ugarte, 2014). En este contexto relativo a la esfera personal del individuo, Gardón Valdes (citado en Ugarte, 2014) plantea en su investigación una distinción entre "lo privado" y "lo íntimo". Mientras que lo primero hace referencia a voluntades y preferencias individuales de alguien, lo segundo entraña algo mucho más discreto pues, según el autor, se trata de *"los pensamientos de cada cual, de la formación de las decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado"*. Por otro lado, otros autores entienden el derecho a la privacidad como un presupuesto esencial unido al derecho a la intimidad (Fraguío, 2018).

Adicionalmente, la doctrina ha delimitado el concepto igualando la privacidad a *"la esfera autónoma de actuación y desarrollo personal"* garantizada por la protección otorgada a los bienes protegidos en el art. 8 CEDH (derechos personalísimos ligados a la existencia del individuo) (Cazurro, 2020).

Habida cuenta lo expuesto, se puede concluir que lejos de acogerse el discutido término en todos sus extremos a la intimidad, abarca este un espacio mayor. En otras palabras, todo lo íntimo (por extensión) es privado, pero no viceversa. En este sentido se pronuncian autores como Pierini, Lorences y Tornabene (citados en Nisa, 2020).

Por consiguiente, ambos conceptos se ven amparados por el derecho a la protección de datos que se analizará a continuación.

- <u>Protección de datos</u>

Como se ha ido exponiendo a lo largo de la investigación, en los últimos años el derecho a la protección de datos está ganando importancia en el terreno de las relaciones laborales.

No obstante, este derecho necesita de una definición conceptual *"innovadora, realista y con capacidad de adaptación"* (Nisa, 2020) que logre abarcar todos los extremos que ha de proteger.

Hasta la fecha se han distinguido cuatro teorías vigentes sobre la protección de datos (*la teoría del mosaico, teoría de las esferas o círculos concéntricos, teoria del "right to privacy" y la "Restricted Access/Limited Control (RALC) Theory of Privacy"*) que no han entrado a analizar en profundidad el ámbito de protección de este derecho (Nisa, 2020).

De las evidencias anteriores se desprende la necesidad de esclarecer en este apartado el concepto de "derecho a la protección de datos".

En primer lugar, se trata de un derecho recogido en el artículo 18.4 de la CE que recibe el nombre de "libertad informática". Asimismo, la jurisprudencia nacional especificó que el derecho a la protección de datos o libertad informática es un derecho fundamental independiente y autónomo (STC 292/2000)[6]. Por lo que, a partir de estas premisas, se ha de discernir ahora su alcance y objeto.

El TC señala que cualquier actividad concerniente a la trata de datos personales de un individuo (íntimos o no) puede resultar una amenaza para él (Martínez, 2007). A partir de esta manifestación es necesario atender a dos términos que configuran la definición de este derecho: "la trata" y "datos". Se trata de dos conceptos que se instauran sobre el derecho fundamental a la protección de datos dotándolo de sentido y protección (Martínez, 2007).

Adicionalmente, en virtud de la sentencia del TC mencionada con anterioridad, el derecho a la protección de datos *"atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley…"* (STC 292/2000). En otras palabras, se trata de un derecho fundamental que concede al individuo la facultad de: otorgar consentimiento para la trata de datos, conocer el destino de estos, impedir su uso inapropiado y acceder a ellos para mantenerlos, rectificarlos e incluso cancelarlos (Martínez, 2007). No obstante, cabe estudiar qué datos son protegidos y cuales no pues, si atendemos solo a la literalidad del texto es muy complejo llegar a una clara conclusión.

En lo referente a su alcance, desde el año 2000 en el que el TC sentó jurisprudencia, las vicisitudes son algo más sencillas. Conviene señalar que el tribunal

[6] Tribunal Constitucional (Pleno). Sentencia núm. 292/2000, de 30 de noviembre de 2000. ECLI:ES:TC:2000:292

delimitó la naturaleza y el objeto del derecho a la protección de datos y lo consagró *"cómo derecho fundamental autónomo, vinculado a la privacidad de las personas, ya que el derecho a la protección de datos no se reduce solo a los datos íntimos de las personas sino 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 solo la intimidad individual, protegida por el artículo 18.1 de la Constitución, sino los datos da carácter personal…"* (STS 1033/2020)[7].

De lo anterior se desprende que el objeto del derecho a la protección de datos o libertad informática es más amplio que aquel que ostenta el derecho a la intimidad (18.1 CE) pues salvaguarda no solo los datos más íntimos, sino cualquier dato personal del individuo. Por lo tanto, estos derechos se diferencian tanto en su función, como en su objeto y contenido.

En relación con el derecho a la protección de datos, resultan de aplicación las siguientes normas: art 18.4 CE[8], art. 8 CDFUE[9], art 16.1 TFUE[10], RGPD y LOPDGDD. De manera análoga, es preciso apuntar que el órgano encargado en España del cumplimiento de la normativa en el territorio es la Agencia Española de Protección de Datos.

- Intimidad

En último lugar, es necesario proceder al estudio del derecho a la intimidad. Se trata de un derecho fundamental regulado en el art 18.1[11] de la CE que cuenta con un objeto menor que el derecho a la protección de datos.

---

[7] Tribunal Supremo. Sentencia núm. 1033/2020, de 25 de noviembre de 2020. Rec. 39/2019. ECLI:ES:TS:2020:4187

[8] Art. 18.4 CE: "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."

[9] Art. 8 CDFUE – Protección de datos de carácter personal: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente."*

[10] Art 16 TFUE: *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."*

[11] Art. 18.1 CE: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".*

Atendiendo a la literalidad del artículo, es confuso determinar si se trata de un solo derecho (derecho a la intimidad) o, por el contrario, coexisten tres diferentes (derecho al honor, derecho a la intimidad y derecho a la propia imagen). Existe mucha polémica al respecto pues, mientras unos autores defienden que la materia de los tres derechos es merecedora de especial e individual atención, otros consideran que han de entenderse de manea conjunta al ser su fundamento es el mismo (Martínez de Pisón, 2016). En la presente investigación se atenderá a la hipótesis referente a la necesidad de individualización de los tres derechos mencionados en el art. 18.1 CE.

Pese a los desconciertos señalados, no debe desatenderse su transcendencia tanto en el plano social, como en lo jurídico. Su relevancia ha ido aumentando en los últimos años debido a los avances tecnológicos ya mencionados en la presente investigación. En este sentido, el derecho a la intimidad "*forma parte de este conjunto de libertades fundamentales vinculadas muy estrechamente a la persona y a la concepción civil y política de la ciudadanía"* y, de igual manera *"supera a otras libertades individuales tradicionalmente mucho más importantes"* (Martínez de Pisón, 2016). *Asimismo, "La intimidad personal y familiar es, en suma, un bien que tiene la condición de derecho fundamental (art. 18.1 de la Constitución) y sin el cual no es realizable, ni concebible siquiera, la existencia en dignidad que a todos quiere asegurar la norma fundamental (art.10.1)"* (STC 20/1992)[12].

Expuesto lo anterior y habiendo quedado clara la transcendencia jurídica del derecho a la intimidad, procede ahora ahondar en la jurisprudencia y concretar la parcela de la vida de una persona que ampara este derecho.

En este sentido, se propone una definición para el concepto de "intimidad": *"ha de subrayarse que la noción de intimidad constitucionalmente protegida es un concepto de carácter objetivo o material, mediante el cual el ordenamiento jurídico designa y otorga protección al área que cada uno se reserva para sí o para sus íntimos, un ámbito reservado de la vida de las personas excluido del conocimiento de terceros en contra de su voluntad"* (STC 170/2013)[13].

[12] Tribunal Constitucional (Pleno). Sentencia núm. 20/1992, de 14 de febrero de 1992. ECLI:ES:TC:1992:20

[13] Tribunal Constitucional (Pleno). Sentencia núm. 170/2013, de 7 de octubre de 2013. ECLI:ES:TC:2013:170

De la mano de lo anterior, el TS dispone que *"el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido. Corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno"* (STS 97/2015)[14].

En efecto, se trata de un derecho que por un lado protege datos íntimos[15] y por otro, otorga al sujeto el derecho de prohibir a terceros la intromisión. No obstante, con el propósito de delimitar más su ámbito de protección, a continuación se analizarán cuáles son los extremos de la vida de una persona que forman parte de su esfera íntima (y por tanto, están protegidos por este derecho).

Según lo concretado en otro pronunciamiento del TS, la esfera íntima se refiere a aquellos datos relativos a la salud, la ideología, la vida sexual o las creencias, entre otros. Este perímetro objeto de protección del derecho a la intimidad personal y familiar es designado por la jurisprudencia como "núcleo duro de la privacidad" (STS 53/2015)[16].

Por ello, se insiste en lo expuesto anteriormente pues, con este argumento se ratifica la idea de que la intimidad forma parte de la privacidad de un individuo pero no viceversa y, ambas se ven protegidas por el derecho a la protección de datos arriba expuesto.

En cuanto a lo que a su regulación se refiere, del derecho objeto de estudio en el presente apartado, destacamos: art. 18.1 CE[17], art. 7 CDFUE[18], art. 8 CEDH[19] y LO

---

[14] Tribunal Supremo. Sentencia núm. 97/2015, de 24 de febrero de 2015. Rec. 1774/2014. ECLI:ES:TS:2015:823

[15] Que según el criterio jurisprudencial se pueden defender como *"conjunto de vivencias, experiencias o rasgos caracteriales exclusivos que cada quien aspira a mantener bajo reserva y para sí, al tratarse de datos que le comprometen de manera intensa, porque son de los que le hacen ser el que es como persona"* (STS 659/2014). En el mismo sentido, la jurisprudencia también lo entiende como "*concepto psicológico que remite a ese "mundo propio" en el que cada quien desarrolla su "vida interior"* (STS 534/2011)

[16] Tribunal Supremo. Sentencia núm. 53/2015, de 23 de septiembre de 2015. Rec. 648/2015. ECLI:ES:2015:3874

[17] Art. 18.1 CE: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*

[18] Art. 7 CDFUE – Respeto de la vida privada y familiar: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".*

[19] Art. 8 – Derecho al respeto a la vida privada y familiar: *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"*

1/1982 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

3. PRINCIPIOS EN MATERIA DE PRIVACIDAD, INTIMIDAD Y PROTECCIÓN DE DATOS.

3.1 Principios constitucionales

Habiendo analizado y comparado los términos anteriores, procede ahora detenerse en los principios constitucionales que la CE recoge en su texto, bien de forma expresa como los establecidos en el art. 9 CE, o bien implícita como el Derecho al Trabajo recogido del art. 35 CE (Puig, 2001).

Pese a que la presente investigación no sigue un análisis constitucional, se ha reparado en la necesidad de analizar de manera general los principios constitucionales básicos. De esta manera, resultará mucho más sencillo entender la resolución de los conflictos en el ámbito laboral que más adelante se contemplarán.

En primer lugar, estos principios garantizan y amparan el ejercicio de cualquier derecho fundamental y, por ende, quedan incluidos el derecho a la intimidad, el derecho a la privacidad y el derecho a la protección de datos.

Por ello, seguidamente se analizarán aquellos principios que influyen directamente sobre los derechos que suponen el núcleo de esta investigación:

- El principio de vinculatoriedad del art. 9.1 CE[20], basado en la sujeción de los ciudadanos y los poderes públicos a la Constitución y al resto del ordenamiento jurídico.

  Este principio también recibe el nombre de "fuerza vinculante" o "eficacia inmediata de los derechos" (Abellán, 2003).

  Este apartado por un lado garantiza un orden de convivencia y por otro, insiste en la supremacía de la Constitución al ser esta la norma más importante del país. Asimismo, sostiene que los poderes públicos han de actuar conforme a la CE y que los ciudadanos deben abstenerse de actuar en contra de lo establecido en esta norma (STC 101/1983)[21][22].

[20] Art. 9.1 CE: *"Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico".*

[21] Tribunal Constitucional (Pleno). Sentencia núm. 101/1983, de 18 de noviembre de 1983. ECLI:ES:TC:1983:101

[22] En el mismo sentido se pronuncia la STC 80/1982, de 20 de diciembre.

En síntesis, el contenido de este artículo es una de las piedras angulares del texto constitucional y por tanto directamente aplicable a las relaciones laborales ya que, ni empleado ni empleador estarán exentos de respetar las normas que componen el ordenamiento jurídico español.

- El principio del art. 9.2 CE[23] relativo al mandato al poder público con el objeto de que éste asegure el cumplimiento de la libertad y la igualdad (real, material o efectiva) de todos los ciudadanos.

  Este precepto sirve como criterio hermenéutico del resto de la norma (Carmona, 2004). Asimismo, tiene proyección sobre el derecho a la intimidad, privacidad y protección de datos ya que, en caso de pleito sobre la materia, la jurisdicción competente deberá asegurar un cumplimiento real y efectivo de la libertad e igualdad de los ciudadanos.

- Los principios articulados en el 9.3 CE[24]: el principio de legalidad (basado en dar con una solución ajustada a derecho), principio de jerarquía normativa (las normas se ordenan en un modo concreto de prelación, hay normas con mayor rango), de publicidad de las normas (los ciudadanos han de conocer las normas y su ignorancia no exime del cumplimiento), de irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales (como regla general, las normas surten efecto a futuro desde su aplicación y nunca hacia atrás), principio de seguridad jurídica (procesos, normas y garantías a disposición del ciudadano).

[23] Art. 9.2 CE: *"Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social".*

[24] Art. 9.3 CE: *"La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos".*

Todos estos principios son trasladables al contexto de las relaciones laborales y, consecuentemente, al derecho a la privacidad, intimidad y protección de datos pues.

- El principio de responsabilidad de los poderes públicos: en relación con este principio se encuentra el art. 106 CE[25].

  En este sentido, en caso de que los derechos a la intimidad, privacidad o protección de datos del trabajador o del empresario sean vulnerados como consecuencia de la mala praxis de los poderes públicos, tendrán derecho a ser compensados.

- El principio de interdicción de la arbitrariedad de los poderes públicos: la prohibición de que un poder público actúe saltándose las normas y procedimientos legales establecidos, principio de respeto al contenido esencial de los derechos fundamentales y principio de aplicabilidad inmediata de los derechos fundamentales.

Expuesto lo anterior, cabe detenerse ahora en el principio de proporcionalidad y el principio de razonabilidad. Ambos conceptos serán referidos en numerosas ocasiones durante la exposición de esta investigación.

- El principio de proporcionalidad guarda especial relación con los derechos fundamentales de las personas (Alexy, 2011). De esta manera, se trata de una herramienta que sirve a los jueces y tribunales para (entre otras cosas) resolver los conflictos entre derechos. A lo largo de la presente investigación se analizará este principio desde la perspectiva de la colisión de derechos del trabajador y del empresario. No obstante, no se puede afirmar que el principio de proporcionalidad tenga como fin último delimitar qué derecho es más importante, pues bien, procura minimizar las lesiones o perjuicios y pondera los derechos en virtud del contexto. En este sentido, establece el TC (citado en Trías, 2013) que *"el principio de proporcionalidad, que exige una relación*

[25] Art. 106 CE: "*Los particulares, en los términos establecidos por la ley, tendrán derecho a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos"*

ponderada de los medios empleados con el fin perseguido, para evitar el sacrificio innecesario o excesivo de los derechos fundamentales (STC 66/1985 [RTC 1985\66]), cuyo contenido esencial es intangible" (STC 50/1995)[26].

- En lo referente al principio de razonabilidad, los autores defienden que "*la exigencia de razonabilidad resulta de especial importancia respecto de la creación de Derecho, en particular del Derecho normativo y del judicial"* (Martínez y Zúñiga, 2011). Por lo expuesto, se puede concluir que el principio de razonabilidad vela por una actuación legal, válida y prudente de los poderes públicos.

Habida cuenta de lo expuesto, es evidente que, pese a ser conceptos similares y haber autores que los equiparan, ambos principios son diferentes y, por tanto, merecedores de tratamiento diferenciado.

Por razones lógicas, todo lo anterior recae sobre los derechos analizados en esta investigación pues se trata de derechos fundamentales garantizados por estos principios.

3.2 Principios básicos en materia de protección de datos

De manera análoga a los principios fundamentales, cabe ahora referirse a principios básicos en materia de protección de datos que la AEPD delimita mediante referencia expresa al RGPD, en concreto a su Capítulo II, Art. 5 (el cual será objeto de desarrollo en las siguientes líneas).

En este sentido, estos principios *"permiten concretar el DPD en la práctica de su ejercicio, así como cuáles son los aspectos, facultades y obligaciones que deben ser observadas en lo relativo al tratamiento de datos"* (Fraguío, 2018).

Estos principios son:

- Licitud, transparencia y lealtad: Art 5.1 RGPD: *"Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado"*.

Con el propósito de profundizar en este apartado, se ha de atender a lo expuesto en el considerando 39 del RGPD. En su redacción se puede observar una división del principio objeto de estudio en dos partes, primero se refiere al "tratamiento licito y leal" y más tarde habla del "tratamiento transparente". Por este motivo, en la presente

[26] Tribunal Constitucional (Pleno). Sentencia núm. 50/1995, de 31 de marzo de 1995. ECLI:ES:TC:1995:50

investigación se seguirá el mismo criterio. No obstante, cabe detenerse en lo expuesto por la jurisprudencia sobre las particularidades de cada elemento.

En primer lugar, el considerando mencionado establece que *"todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados".* En este sentido, para garantizar una trata lícita, se ha de atender a lo dispuesto en el art. 6 RGPD[27] pues en él se detallan las condiciones necesarias para estimarlo como tal. Como se ha adelantado, en el RGDP la lealtad acompaña a la licitud, sin embargo, si se pretende delimitarlo de manera individual, cabe apuntar que en la jurisprudencia laboral el término "lealtad" se ha venido asociando a la buena fe.

Por otro lado, continuando con el análisis del considerando 39 RGPD, se dispone que *"el principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento".* En este sentido, se

[27] *Art. 6.1. RGPD: El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

entiende por garantía de transparencia la "*obligación de información útil o de calidad*" por parte del empresario a los trabajadores (STSJ 566/2021)[28].

Habida cuenta lo anterior, cabe apuntar que ciertos autores no siguen esta diferenciación, sino que advierten que la literalidad del art. 5.1 c) se trata de "*un trimonio*" de principios que han de ser tratados como un todo (Olivares, 2021).

- Finalidad: Art 5.1 RGPD: *"Los datos personales serán: b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines…"*

Según la aclaración realizada por la AEPD, este principio tiene doble objeto pues, por un lado, se pretende asegurar que la trata de datos sea llevada a cabo con uno más fines concretos y, por otro, que esta se ajuste a tales fines y sea congruente con los mismos. En otras palabras, *"pretende evitar, a toda costa, la recogida de datos de manera indiscriminada sin contar con ninguna finalidad, finalidad que debe ser definida previamente a la recogida de datos"* (García-Poveda, 2018).

Habida cuenta la importancia de este principio, autores consideran que ha de ser distinguido frente al resto pues *"supone un presupuesto preliminar que resultará idóneo para evaluar cada práctica operada en este terreno"* (Fraguío, 2018).

En este sentido, atendiendo al contexto de las relaciones laborales, cualquier otra finalidad alejada en lo establecido en el art. 20.3 ET[29] podría resultar abusiva para el trabajador y, el empresario estaría excediéndose en sus competencias.

- Minimización de datos: Art 5.1 RGPD: *"Los datos personales serán: c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".*

Lo que pretende la norma es reducir lo máximo posible el número de datos recogidos para la trata, y acotarse o ceñirse exclusivamente a aquellos que resulten estrictamente necesarios para el cumplimiento de los fines delimitados. Es por esto por lo

[28] Tribunal Superior de Justicia de Andalucía, Málaga. Sentencia núm. 566/2021, de 24 de marzo de 2021. Rec. 316/2021. ECLI:ES:TSJAND:2021:5399

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

que en las siguientes líneas se centrará el foco de estudio en analizar qué requisitos son necesarios para cumplir con el precepto.

En primer lugar, es difícil fijar reglas matemáticas sobre lo "estrictamente necesario" si bien es cierto, "necesario" no puede entenderse sinónimo de "conveniente" (Álvarez, 2021). De esta manera, en caso de que sea preciso delimitar este concepto, serán en cada caso los tribunales los encargados de ponderar las circunstancias en juego que justifiquen o no la trata.

En segundo lugar, este principio "*implica que los datos innecesarios a la finalidad perseguida por el agente no podrán ser recogidos y almacenados sólo porque pudieran resultar útiles con posterioridad*" (Montoro, 2015).

Finalmente, cabe señalar que en la jurisprudencia analizada los tribunales españoles vinculan la minimización de datos al "principio de proporcionalidad". En este sentido, los hechos serán sometidos al "*test de proporcionalidad*" por medio del triple filtro de idoneidad, necesidad y proporcionalidad (SJS de 18 de noviembre de 2021)[30].

- Exactitud: Art 5.1 RGPD: *"Los datos personales serán: d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)".*

Asimismo, este principio se encuentra recogido y desarrollado en el art. 4 de la LOPD.

En primer lugar, atendiendo al contenido del principio, procede establecer una diferencia entre "exactitud" y "actualización" pues, mientras que todos los datos desactualizados sí son considerados datos inexactos, no se puede garantizar que los datos actualizados sean exactos (Maroto, 2018).

De igual modo, cabe plasmar la diferencia entre el "derecho de supresión" y el "derecho de rectificación" mencionados en el propio principio. Por un lado, el derecho de supresión o derecho al olvido del art. 17 del RGPD[31] faculta al interesado (trabajador

[30] Jugado de lo Social núm. 26 de Barcelona. Sentencia de 18 de noviembre de 2021. Procedimiento núm. 177/2020. ECLI:ES:JSO:2021:7119

[31] Art. 17 RGPD - Derecho de supresión («el derecho al olvido»): *"1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en*

en un contexto laboral) para exigir la supresión de datos personales (al empresario) siempre y cuando cumpla con las condiciones necesarias para ello que están dispuestas en el propio artículo. Por otro lado, el derecho de rectificación está recogido en el art. 16 del RGPD[32] y tiene por objeto conferir al interesado el derecho a corregir y/o completar sus datos personales.

Procede apuntar que no podrá atribuirse la culpa de la inexactitud de los datos al encargado del tratamiento, en caso de este que haya tomado las medidas razonables para que estos se suprimen o rectifiquen (Maroto, 2018).

Si de manera análoga, si se traslada lo expuesto al seno de las relaciones laborales, se puede afirmar que el empresario debe aplicar todas las medidas que estén a su disposición para garantizar que los datos de los trabajadores sean correctos y actualizados. De igual manera, el trabajador tiene derecho a suprimir y/o rectificar la información inexacta sobre su persona en el menor tiempo posible.

- Limitación del plazo de conservación: Art 5.1 RGPD: *"Los datos personales serán: e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos*

que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. 2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. 3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones".

[32] Art 16 RGPD – Derecho de rectificación: *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional"*

personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»).

No se puede hablar de plazo máximo exacto en virtud del cual el encargado de la trata de datos puede conservarlos. No obstante, tampoco existe libertad total para la conservación o mantenimiento de estos pues, en virtud de lo establecido por la ley, no se podrá disponer de los datos más tiempo del necesario para la consecución del fin determinado por el que fueron almacenados.

Si bien esto es cierto, cabe apuntar que es considerado uno de los principios más complejos pues resulta muy complicado conocer cuándo un dato deja de ser útil (Olivares, 2021).

No obstante, el artículo enumera situaciones en las que se permite la conservación de los datos durante periodos más prolongados en el tiempo. Sin embargo, si se atiende a su literalidad, son mínimas las situaciones en las que esto está permitido.

En el contexto de la contratación laboral, los empresarios no podrán mantener bajo su poder los datos de sus trabajadores cuando haya extinguido el fin por el que fueron recogidos. Como se ha venido exponiendo a lo largo de la presente investigación, el derecho a la protección de datos es un derecho fundamental de las personas (y por lo tanto de los trabajadores). Por ello, no es posible excederse en la conservación de datos relativos a las personas pues de lo contrario, no se estaría garantizando el respeto a este derecho.

Una vez analizado el contenido del principio, cabe señalar que la limitación del plazo de conservación está directamente relacionada con el principio de finalidad. En este sentido, se trata de dos aspectos que han de ser considerados en toda trata (AEPD, 2019).

El encargado de la trata deberá determinar el tiempo máximo de trata de datos en función de la finalidad para los que son empleados (Olivares, 2021). Por tanto, cabe subrayar que no es la AEPD sino el propio fin el cual determinará el tiempo máximo de preservación de datos.

Llegado a término el periodo de conservación razonable, "*los datos deben ser borrados, bloqueados o, en su defecto, anonimizados*" (AEPD, 2021). Insiste la doctrina que la trata de datos excedida en el tiempo *"carece de razón de ser*".

- Seguridad: Art 5.1 RGPD: *"Los datos personales serán: f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."*

De la literalidad del artículo procede mencionar tres conceptos fundamentales: "seguridad", "integridad" y "confidencialidad". No obstante, con el fin de realizar una aproximación más detallada de la relación de estos tres elementos, se ha de añadir el término "disponibilidad" (tan usado por la doctrina durante el estudio de este principio).

Los conceptos mencionados se relacionan entre sí, pudiendo considerar que *"el concepto de seguridad debe abarcar tanto la confidencialidad de la información como la disponibilidad e integridad de la misma"* (Garriaga, 2016).

Primero de todo, la disponibilidad hace referencia a la capacidad de las personas facultadas a acoger los datos en el tiempo convenido. Asimismo, la integridad se refiere a que dichos datos no han de ser manipulados o perdidos. Y finalmente, la confidencialidad asegura que solo conozcan de ellos las personas acreditadas (Garriaga, 2016).

Habida cuenta lo expuesto, el contenido del principio de seguridad de los datos en el contexto de las relaciones laborales es hoy una cuestión de vital importancia. Quienes lleven a cabo la trata de datos, deberán servirse de los regímenes necesarios para garantizar la seguridad de estos.

Adicionalmente, entre las potenciales medidas empleadas para cumplir con este principio, puede resultar necesario la designación de un Delegado de Protección de Datos en la empresa. Esta figura *"es el garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control (AEPD)"* (Palomar y Fuertes, 2022).

No obstante, pese a ser evidente que el DPO facilita la trata segura, minimiza los riesgos y vela por la información y el cumplimiento de los principios objeto de análisis en el presente apartado, no siempre resulta necesaria su presencia. Generalmente se exige

únicamente en empresas internacionales, grupos de empresas, entidades públicas u otro tipo de organizaciones de gran escala.

Por último, el incumplimiento de la seguridad en la trata de datos en el contexto de una relación laboral pondrá en entredicho el ejercicio de la empresa. Asimismo, será sancionada según lo establecido en la ley y jurisprudencia. Para evitar tal escenario y asegurar primero sortear cualquier potencial vulneración de derechos fundamentales, cabe insistir en la utilidad que conlleva contar con un experto (interno o externo) en la materia que (conviviendo con la figura del DPO) ratifique que el empresario cumple con el principio de responsabilidad activa que sigue a continuación.

- Responsabilidad activa o demostrada: Art 5.2 RGPD: *"El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."*

En caso de litigio o inspección por parte de la AEPD, el encargado de la trata deberá estar capacitado para no solo testificar que obedece y acata el reglamento y demás normativa, sino que tendrá que poder probar tal honesta y diligente actuación. Es precisamente esta posibilidad de manifestación del cumplimiento o diligencia lo que se conoce por "responsabilidad proactiva".

En el mismo sentido, *"en la práctica, lo mencionado supone que las empresas y profesionales han de habilitar procesos de análisis, evaluación y acreditación (previa identificación de tipología de los datos que tratan, finalidades y operaciones o actividades que comprende dicho tratamiento). Y en congruencia con ello, han de informar sobre el sistema de tratamiento y los medios empleados, de forma que además puedan probar que las medidas adoptadas son las adecuadas ante los interesados y las autoridades de supervisión"*. (Fraguío, 2018).

Atendiendo a la disposición del artículo que se viene estudiando, cabe detenerse en el hecho de que el principio de responsabilidad proactiva se encuentra diferenciado en un apartado concreto y, por tanto, separado del resto de principios analizados. De ello se concluye que es merecedor de una atención especial. Según lo establecido en la doctrina "*si bien no es una definición en sí misma, de la literalidad de la norma sí cabe desprender que la responsabilidad proactiva es la obligación para todo responsable del tratamiento de demostrar el cumplimiento de los principios de: minimización de datos, exactitud, confidencialidad y seguridad, limitación de la finalidad y limitación del tiempo de*

conservación" (de Marcos, 2021). En definitiva, este principio abarca todos los anteriores, ya que no persigue otra cosa que poder justificar que cumple con lo dispuesto en el primer apartado del artículo.

En definitiva, mediante presente estudio se corrobora que, sobrepasar los limites que el reglamento y los principios imponen, puede resultar más sencillo de lo que habitualmente se presume. Entre tantos motivos, se debe al avance en los mecanismos de control laboral, las nuevas tecnologías y redes sociales, y el contexto actual. Como se ha adelantado en líneas anteriores, el Derecho Laboral es algo muy vivo hoy día (un ejemplo claro ha sido la crisis de la COVID-19 en esta área) y, por tanto, es importante enfatizar en la transcendencia de la actualización de las normas y sus interpretaciones.

4. PRINCIPALES MECANISMOS DE CONTROL LABORAL

El empresario, en el ejercicio del poder de dirección que le atribuye el Estatuto de los Trabajadores y directamente relacionado este poder con el derecho a la libertad de empresa recogido en el art. 38 CE, es el habilitado para: impartir órdenes sobre los diferentes extremos que alcanza la prestación de trabajo (lugar, tiempo, forma, entre otras), establecer y modificar las condiciones de su empresa, hacer cumplir las obligaciones u órdenes e imponer sanciones si fuera necesario, controlar y vigilar a los empleados que configuran la plantilla, e incluso cerrar el centro si se cumplieran los requisitos necesarios para ello.

En otras palabras, la doctrina considera que lo que se conoce por "poder de dirección" del empresario, es un concepto que abarca a su vez tres facultades distintas: el poder ordinario del empresario, el ius variandi empresarial y el poder de vigilancia, control y sancionador (Fabregat, 2016).

No obstante, dichos poderes no son absolutos o preferentes. Como en toda relación contractual, existen dos partes y en las contrataciones laborales son los propios trabajadores de la empresa quienes constituyen verdaderos límites a la condición de empresario.

En la presente sección se estudiarán los medios por los que el empresario empleador ejerce su poder de control y vigilancia conferido por la ley. Asimismo, se analizarán las posibles colisiones de dicha facultad con lo que respecta a la dignidad del empleado.

Cosa distinta al objeto de análisis en las siguientes líneas son las medidas adoptadas por el empresario en situaciones de urgencia. En estos casos, el empresario tiene la extraordinaria necesidad de instalar mecanismos de control perentoriamente por existir indicios que lo justifiquen (sospechas de hurto, incumplimiento de la buena fe…).

Habida cuenta lo expuesto, a continuación se describirán los principales mecanismos de control ordinario llevados a cabo por el empresario en el contexto de las relaciones laborales.

4.1 Ordenador del trabajador

Los ordenadores, en virtud de su plurifuncionalidad, facultan a cualquier persona no solo a desarrollar actividades profesionales relativas a su condición de empleado y/o

estudiante, si no que también se utilizan como medio para llevar a cabo movimientos referentes a su esfera privada (indagar en las redes sociales, descargar archivos o imágenes personales, mantener conversaciones personales a través de distintas vías de comunicación como WhatsApp web, Telegram…).

No obstante, cuando el ordenador es proporcionado por el empresario en el contexto de una relación laboral, el empleador (amparado por el Estatuto de los Trabajadores) está facultado para monitorizar los ordenadores y conseguir de esta manera un control más estricto.

A consecuencia de lo anterior, es posible que nazcan problemas entre las partes de la relación jurídico laboral. De esta manera, no es extraño que, debido a un uso personal del ordenador del trabajo y un mínimo control por parte del empresario, se hayan vulnerado derechos fundamentales del trabajador. Por consiguiente, es importante hacer hincapié en que los propios trabajadores personifican un limite a los poderes del empresario y, en este caso particular, a la facultad de dirección y control.

Si bien esto es cierto, la situación era mucho más compleja hasta la entrada en vigor de la LOPDGDD en diciembre de 2018. Hasta ese momento solo existían opiniones sobre lo que podría hacerse y lo que no. Pues bien, hay quienes consideraban que el empresario tenía total libertad para acceder a la información de sus trabajadores al ser las herramientas de trabajo de su propiedad. Mientras tanto, otros pensaban que de ninguna manera el empresario podría llegar a recopilar información íntima de sus trabajadores (Delgado, 2020).

Para para solventar esta problemática la jurisprudencia se ha pronunciado al respecto en numerosas ocasiones llegando a un punto intermedio entre las dos posturas expuestas (Delgado, 2020). De esta manera, se defiende que para que la monitorización de los ordenadores de los trabajadores no suponga una intrusión en su esfera íntima, el empresario deberá informar a toda la plantilla (independientemente del rango a ocupar) sobre la prohibición del uso del ordenador de la empresa con fines personales. Esta información será expresa e inequívoca.

En línea con lo expuesto, la jurisprudencia nacional insiste en la importancia de asegurar que los trabajares conozcan tal prohibición y afirma que *"en estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente*

sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad" (STS de 6 octubre de 2011)[33].

Además de informar sobre tal prohibición, en caso de que el empresario decida puntualmente ejercitar el poder de control del que dispone por ley, la jurisprudencia (STSJ 2716/2010)[34] *"es necesario que previamente se haya advertido a los representantes de los trabajadores y a los propios trabajadores de la existencia de un mecanismo de control respecto el uso de los medios informáticos, así como de las consecuencias que se pueden derivar de un uso abusivo de los mismos"* (Fabregat, 2016).

Recientemente el TSJ se ha pronunciado respecto la necesidad de comunicación fijando que *"con la finalidad de salvaguardar el derecho a la intimidad que tiene el trabajador, éste tiene que ser advertido de la posibilidad de que sus comunicaciones pudieran ser objeto de seguimiento y control por la empresa"* (STSJ 88/2022)[35]. Asimismo, establece la sentencia que un pacto de confidencialidad no equivale nunca a una advertencia sobre la intención de ejercer control empresarial. Esta afirmación ha de ser considerada por los empleadores antes de proceder a la intervención del ordenador de sus trabajadores (Esteban, 2022).

De manera análoga, de lo deducido en la jurisprudencia se puede concluir que incluir una cláusula con el contenido de la prohibición en el convenio es necesario, pero no suficiente. Lo idóneo para demostrar absoluta intransigencia a este tipo de actuaciones sería trasladar la comunicación por escrito a los trabajadores, asegurándose de que estos firman y aceptan dicha condición. De esta manera, se cumpliría con el principio de autotutela informativa que vela por el cumplimiento de *"la obligación de recabar el consentimiento de las personas afectadas para el tratamiento y utilización de la información que les concierna"* (Del Pozo y Mañá, 1996).

Por todo lo expuesto, en definitiva, para proceder a controlar el ordenador del trabajador, el empresario deberá: en primer lugar, informar (si procede) sobre la prohibición de utilización del ordenador para fines personales y, en segundo lugar, informar sobre los medios de control adoptados.

[33] Tribunal Supremo. Sentencia de 6 de octubre de 2011. Rec. 4053/2010. ECLI:ES:TS:2011:8876
[34] Tribunal Superior de Justicia de Valencia. Sentencia núm. 2716/2021, de 5 de octubre de 2010. Rec. 2195/2010. ECLI:ES:TSJCV:2010:7242
[35] Tribunal Superior de Justicia de la Región de Murcia. Sentencia núm. 82/2022, de 26 de enero de 2022. Rec. 754/2021. ECLI:ES:TSJMU:2022:35

4.2 Correo electrónico

Entrando ahora en el caso particular del correo electrónico, cabe apuntar que, del mismo modo en el que el ordenador es comúnmente utilizado con fines extralaborales, es fácil que el correo electrónico se emplee como medio de comunicación personal.

Este tipo de comunicaciones pueden formar parte de la intimidad de una persona pues dependerá de la delimitación que su titular haga al respecto. En este sentido, *"esfera de la intimidad personal está en relación con la acotación que de la misma realice su titular, habiendo reiterado este Tribunal que cada persona puede reservarse un espacio resguardado de la curiosidad ajena"* (STS 678/2014)[36].

Si bien es cierto, pese a tratarse de un asunto complejo, habrá que considerar la gravedad de las actuaciones, su tipicidad y la proyección en la productividad del empleado, entre otros aspectos.

Por ende, es preciso señalar que, en el escenario de un conflicto por un inadecuado uso del correo electrónico no existe una solución unánime y es fundamental analizar las particularidades del caso concreto y realizar un juicio de proporcionalidad (STC 170/2013)[37].

De esta manera, el pasado 5 de septiembre de 2017 la Gran Sala se pronunció al respecto mediante la resolución del Caso *Bârbulescu II* contra los tribunales rumanos. Este versaba sobre la posibilidad de control empresarial en comunicaciones electrónicas de un trabajador y el impacto en su derecho a la privacidad. En este sentido, el tribunal ponderó tanto los intereses en juego como los antecedentes del caso. Al ser el contenido del pronunciamiento notablemente extenso, nos centraremos en las conclusiones más relevantes:

- Por un lado, se insistió en la importancia de interpretar el concepto "vida privada" desde una perspectiva amplia. De esta manera, lo privado no se debe reducir a lo íntimo y abarca la "vida privada social". Consecuentemente, las comunicaciones electrónicas en el contexto laboral han de ser protegidas bajo este concepto,

[36] Tribunal Supremo. Sentencia núm. 678/2014, de 20 de noviembre de 2014. Rec. 3402/2012. Rec. 3402/2012. ECLI:ES:TS:2014:5215

[37] Tribunal Constitucional (Pleno). Sentencia núm. 170/2013, de 7 de octubre de 2013. ECLI:ES:TC:2013:170

garantizándose así el art. 8 CEDH[38]. No obstante, no significa que este derecho no pueda verse en parte limitado por los intereses del empresario.

- Por otro lado, el tribunal insiste en la importancia del respeto a los principios generales (estudiados en líneas anteriores) e insiste en ser especialmente cuidadoso en los siguientes aspectos: informar al trabajador de manera clara y anterior a la intromisión tanto sobre la posibilidad, como sobre la aplicación de medidas para revisar sus comunicaciones y correspondencia; haber examinado pertinentemente el alcance de la vigilancia y el grado de intromisión en la vida privada del trabajador; aportar razones legítimas fundamentadas (y no solo teóricas) que justifiquen la práctica; determinar que no existían medios menos invasivos para alcanzar tal fin; y por ultimo, acreditar que se ha tenido en cuenta el impacto que el ejercicio de control y la posterior sanción han tenido en el trabajador (Rojo, 2017)[39].

- Finalmente, al entender que el desde el punto de vista de la realidad práctica el empresario no había cumplido con los requisitos anteriormente mencionados, el tribunal considera que se ha vulnerado el art. 8 CEDH y que, por tanto, ha existido intromisión en la vida privada del trabajador (Rojo, 2017).

Repasando ahora el criterio jurisprudencial nacional concerniente al presente campo de estudio, se llega a la conclusión de la importancia de analizar el *Caso Inditex.*

En resumidas cuentas, la empresa había despedido a un trabajador tras poner en marcha una auditoria informática sobre ciertos de sus correos con proveedores externos, pues resultaban notablemente sospechosos para la compañía. Posteriormente, el trabajador ejercitó acciones cuestionando la validez de las pruebas.

En primer lugar, el Juzgado de lo Social declara la procedencia del despido. Más tarde, el TSJ confirma la palabra del JS, pero advierte que la prueba es ha de ser declarada nula al vulnerar esta el derecho a la intimidad del trabajador. Luego, debido al descontento del fallo, las partes recurren al TS que se pronuncia con fecha 8 de febrero de 2018. A juicio de esta parte, el tribunal admite el recurso de la empresa sobre la validez de la

[38] Aspecto mencionado con anterioridad en la STEDH del 3 de abril de 2007.
[39] En el mismo sentido se pronuncian los autores José Luis Monereo Pérez y Pompeyo Gabriel Ortega Lozano en su obra "*El control empresarial del correo electrónico del trabajador*" (2019).

prueba. Para resolver la cuestión, aplica tanto la doctrina del TC (STC 170/2013)[40] como la expuesta en el TEDH mediante la resolución del Caso *Bârbulescu II* analizado en líneas anteriores. Finalmente, habida cuenta las sospechas, el examen selectivo y el respeto a proporcionalidad, el tribunal dicta sentencia pronunciándose sobre la validez de la prueba (Navarro, 2020).

Como es lógico, cabe adelantar que sólo podrá ser aportado como prueba en un procedimiento aquellos correos que no vulneren el derecho a la intimidad u otros derechos fundamentales (Delgado, 2022). Esta realidad se desprende de lo estipulado en el art. 11.1 LOPJ que se estudiará en líneas siguientes.

Finalmente, en virtud de lo establecido por expertos en la materia, las nuevas tecnologías y la prohibición de su uso extraprofesional *"es un tema construido a golpe de sentencias"* (Navarro, 2020).

4.3 Historial de navegación

El historial de navegación es merecedor de especial atención pues a diferencia de lo expuesto en relación con los ordenadores y el correo electrónico de la empresa, acceder al historial del trabajador supone casi siempre un quebrantamiento de su derecho a la intimidad (18.1 CE).

No obstante, hay autores que prefieren equiparar y tratar indistintamente estos sistemas de información. De este modo, se defiende que *"la problemática generada por las mismas es común y las sentencias recaídas sobre los tres temas forman parte de una única línea jurisprudencial"* (Delgado, 2020). No obstante, en las siguientes líneas se ejecutará un estudio individual de lo referente al historial de navegación, y se estudiará, si lo hubiera, las diferencias respecto de los medios anteriormente mencionados.

En virtud del art. 8 CEDH, los registros de las páginas buscadas en la web forman parte de la esfera íntima del empleado, pues es frecuente que versen sobre aspectos como: la salud, ideología, vida sexual o creencias (STS 53/2015)[41].

En el mismo sentido se ha pronunciado el TS afirmando lo siguiente: *"pero hay que entender que estos archivos también entran, en principio, dentro de la protección de*

[40] Tribunal Constitucional (Pleno). Sentencia núm. 170/2013, de 7 de octubre de 2013. ECLI:ES:TC:2013:170

[41] Tribunal Supremo. Sentencia núm. 53/2015, de 23 de septiembre de 2015. Rec. 648/2015. ECLI:ES:2015:3874

la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa" (STS 26 se septiembre de 2007)[42].

Por lo tanto, se llega a una primera conclusión ya adelantada en el comienzo de este apartado y es que, mientras que las conversaciones por correo pueden o no formar parte del núcleo íntimo de un individuo (delimitado por él), es prácticamente imposible que la información recogida en el historial de navegación no sea íntima. De esta manera, el empresario deberá ser especialmente cuidadoso en este espacio.

Habida cuenta lo expuesto, cabe resaltar que el empresario tiene un papel especialmente importante en este contexto. El TS continua advirtiendo que *"lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones"* (STS 26 se septiembre de 2007).

Por tanto, evitar la posibilidad de que el trabajador acceda a páginas de internet no necesarias para la prestación de servicios es fundamental para no vulnerar su derecho a la intimidad.

No obstante, en relación con lo anterior, cabe destacar las recomendaciones elaboradas por el Grupo de trabajo el pasado 2002. Estos, además de insistir a los empleadores sobre la importancia de informar a sus trabajadores sobre las condiciones de uso, las prohibiciones y la advertencia del ejercicio del poder de control, también aconsejan no impedirles acceder a búsquedas personales en internet en ningún caso (Delgado, 2020). Es decir, se trata de establecer un equilibrio para que, por un lado, los trabajadores respeten las órdenes no desorbitadas de su empresario y, por otro, que este tenga, poder de control sobre ellos si actúa legítimamente.

Adicionalmente, atendiendo un caso reciente, resulta preciso mencionar la palabra del TSJ de Andalucía del pasado 13 de junio de 2019. En este caso, una empresa despidió a un trabajador por acceder durante la jornada a páginas de contenido sexual, apuestas y

[42] Tribunal Supremo. Sentencia de 26 de septiembre de 2007. Rec. 966/2006. ECLI:ES:TS:2007:6128

otros asuntos ajenos a la empresa (Del Rosal, 2019). Posteriormente, el tribunal declaró que se habían vulnerado los derechos fundamentales del trabajador al no haberse comunicado la intervención del historial de navegación ni tampoco prohibido tales actuaciones (STSJ 905/2019)[43].

Finalmente, lo expuesto ratifica la importancia de una actitud diligente y cuidadosa por parte del empresario.

4.4 Cámaras de videovigilancia

En primer lugar, cabe destacar que son muchos los autores que han estudiado la videovigilancia como sistema de control empresarial. Por ello, se considerará su palabra con el propósito de entender las particularidades del mecanismo.

En este sentido, la Real Academia Española define el concepto de "videovigilancia" como "*vigilancia por medio de un sistema de cámaras, fijas o móviles*". En el ámbito empresarial se traduce como un medio auxiliar a los tradicionales, a través del cual el empleador podrá desempeñar su poder de control.

En otras palabras, "*la videovigilancia permite la captación, y en su caso la grabación, de información personal en forma de imágenes. Cuando su uso afecta a personas identificadas o identificables esta información constituye un dato de carácter personal a efectos de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal (LOPD)[44]"* (Martínez, 2016).

Asimismo, se trata de una cuestión sustancial, merecedora de especial atención por su auge y vigencia en el ámbito del Derecho Laboral (Tillería, 2019).

En las siguientes líneas se analizarán las exigencias necesarias a considerar en caso de que el empresario tenga el propósito de implantar este tipo de medida.

Primero, se ha de apuntar que es una medida cuya regulación y requerimientos cambian frecuentemente. Dicho de otra manera, está sometida a una gran controversia y múltiple criterio jurisprudencial que no es siempre unánime.

[43] Tribunal Superior de Justicia de Andalucía, Sevilla. Sentencia núm. 905/2019, de 28 de marzo de 2019. Rec. 744/2018. ECLI:ES:TSJAND:2019:1355

[44] Derogada por la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDDG).

A continuación, con el fin de disponer de una visión lo más actualizada posible, se hará expresa mención a cuestiones específicas, como el *Caso López Ribalda*, ya que ha supuesto un cambio transcendental en el presente campo.

En cuanto a las exigencias que comporta la videovigilancia como medio para ejercitar el poder empresarial, la AEPD, las leyes concernientes a la materia y los órganos jurisprudenciales han considerado necesarios los siguientes aspectos:

- Que después de haber estudiado en profundidad la viabilidad de la instauración de otro tipo de control menos lesivo, se haya llegado a la conclusión de que la videovigilancia es la opción mejor (o menos gravosa para la intimidad del trabajador) para la situación empresarial de ese momento.

- Que las cámaras sean establecidas en los lugares en los que los trabajadores lleven a cabo la prestación laboral, es decir, no más allá del espacio delimitado para ello (como vestuarios, baños, patios…). Además, salvo que la orientación del establecimiento permitiera otra cosa, no podrá grabarse más allá de este pues se trata de lugares cuya protección queda al amparo de otras autoridades.

- Que se cumplan con los principios descritos en el punto tercero (finalidad, minimización, seguridad…) en todos sus extremos.

- Que exista proporcionalidad entre el fin que justifique la medida, el modo en el que esta se implementa y se tratan las imágenes.

- Si el empleador lo prefiere, podrá nombrar a un encargado para la implantación y regulación de la medida.

- Que el empresario informe a los empleados de la existencia de cámaras por cualesquiera medios (carteles, notificaciones informativas individuales…). Este aspecto es fundamental y la base de la controversia actual. Es común que los empresarios quieran vigilar mediante cámaras, y sin el conocimiento de sus trabajadores, el comportamiento de naturaleza irregular de alguno de ellos. No obstante, la videovigilancia secreta colisiona con el deber de información del

empresario. Por lo anterior, es importante que para que su implantación sea legítima concurran los siguientes requisitos:

- Que haya sospechas razonables de graves irregularidades que supongan perjuicio al empresario. Como su propio nombre indica, no es suficiente la concurrencia de leves indicios de hurto u otras actuaciones anómalas si no que han de ser conjeturas fundadas.

  La Gran Sala se pronunció al respecto en la conocida "Sentencia del asunto López Ribalda II" que concluye de manera contraria a su anterior ("Sentencia del asunto López Ribalda I"). En esta se exterioriza la legitimación de la videovigilancia secreta por entender que existía justificación evidente para que la empresa tomara tal decisión. De esta manera, entre algunos de sus argumentos respaldó la medida justificando lo siguiente: *"En efecto, no era una mera sospecha, sino que las sospechas eran razonables con pérdidas significativas para el empresario"* (STEDH 17 octubre de 2019)[45].

- Que de ningún modo sea un abuso de poder, si no que se justifique (al igual que en la videovigilancia informada) la existencia de un fin legítimo, la exactitud de las medidas y la limitación en el tiempo de estas.

No obstante, es preciso apuntar que la legalidad de la videovigilancia secreta no está recogida en la actualidad en ninguna parte de la legislación española. En líneas generales, se considera que supondría una gran desprotección al trabajador (contingencia que en todo caso el ordenamiento pretende evitar). En este sentido algunos autores afirman que *"podemos sostener que los razonamientos jurídicos consagrados en la sentencia López Ribalda II vienen a establecer un serio retroceso en materia de garantías a la privacidad de las personas físicas, específicamente en el espacio de trabajo"* (Tillería, 2019).

Aunque el pronunciamiento de la Gran Sala haya supuesto una novedad en el deber de información a los trabajadores, no se ha de olvidar que se trata de un contexto

[45] Tribunal Europeo de Derechos Humanos. Sentencia de 17 de octubre de 2019. Caso López Ribalda II contra España. ECLI:CE:ECHR:2019:1017JUD000187413

en el que pueden darse situaciones de inseguridad jurídica en los trabajadores. Por lo expuesto, es preciso reflexionar las circunstancias de cada caso concreto y actuar con prudencia pues, el tribunal competente no aceptará ni un mínimo de desproporcionalidad.

Por último, a partir de este momento será necesario estar al corriente tanto de nuevas interpretaciones jurisprudenciales, como de las posibles novedades legislativas que traiga consigo el dinamismo del Derecho Laboral en relación con la materia expuesta.

5. PODERES DEL EMPRESARIO DURANTE LA PANDEMIA

Con la llegada de la pandemia provocada por la aparición del COVID-19 en marzo de 2020 y ante la alarmante incidencia sanitaria, el país se vio desafiado a enfrentar un sinnúmero de retos tanto en el plano social y político-económico como en muchas de las cuestiones jurídicas con incidencia directa en la sociedad. Este último punto es el que se estudiará en la presente sección del trabajo, pues tiene como propósito analizar las facultades del empresario en el seno de una relación contractual durante la incertidumbre y los cambios normativos fruto de la pandemia.

El confinamiento de marzo de 2020 fue declarado inconstitucional el pasado mes de julio de 2021 (STC 148/2021)[46]. El motivo de tal fallo reside en haberse suspendido derechos fundamentales de gran calibre e importancia por medio del estado de alarma, herramienta no competente para tal medida[47]. Dicho de otra manera, no se juzga a las autoridades por adaptar las medidas alcanzadas en aquella época (pues la emergencia sanitaria requería de las mismas) si no que se objeta el medio a través del cual estas fueron implementadas. Indica el tribunal que el encaje correcto hubiera sido optar por el estado de excepción, sistema que necesita de la autorización del Parlamento y aprobación posterior del Ejecutivo. Adicionalmente, a modo de correctivo, se decidió optar por el reintegro de las sanciones impuestas durante dicho periodo y no atribuir responsabilidad patrimonial al Estado por la paralización de casi toda actividad.

Entre los derechos fundamentales (de carácter limitado y no absoluto) que se vieron afectados, podemos destacar: el derecho a la libertad de circulación, el derecho a la libertad de reunión y manifestación, el derecho a la privacidad o el derecho a la protección de datos de carácter personal (Timón, 2021). Todos ellos colisionaban con el derecho a la salud pública y los intereses vitales de las personas que se vieron amenazados ante dicha contingencia.

---

[46] Tribunal Constitucional (Pleno). Sentencia núm. 148/2021, de 14 de julio de 2021. ECLI:ES:TC:2021:148

[47] Véase: *"Así pues, y por lo que hace específicamente a su posible incidencia en los derechos fundamentales, la declaración de un estado de alarma no consiente la suspensión de ninguno de los derechos de tal rango (que sí cabe para determinados derechos en el supuesto de proclamación del estado de excepción o el de sitio, conforme a los arts. 55.1 y 116.3 y 4 CE), pero sí "la adopción de medidas que pueden suponer limitaciones o restricciones" a su ejercicio (STC 83/2016, FJ 8), que habrán de atemperarse a lo prescrito en la LOAES y a las demás exigencias que la Constitución impone".* (STC 148/2021).

Profundizando en lo que se refiere al derecho de la protección de datos, privacidad e intimidad de la ciudadanía y el contexto de emergencia sanitaria, cabe subrayar que la Orden SND/297/2020, de 27 marzo, encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. Entre estas medidas delegadas se encuentran: en primer lugar, el *"desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos"* (Primero, Orden SND/297/2020) y, en según lugar*, "un estudio de la movilidad aplicada a la crisis sanitaria a través del cruce de datos de los operadores móviles"* (Segundo, Orden SND/297/2020). En resumen, medidas basadas en la geolocalización (tanto social como geográfica) y creación de apps de salud e información sanitaria.

La misma orden, en su disposición cuarta asegura que *"lo dispuesto en esta orden se entiende sin perjuicio de la aplicación del régimen previsto en el 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; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y los criterios interpretativos dados por la Agencia Española de Protección de Datos".* Sin embargo, ha sido objeto de considerable controversia tanto durante el punto más álgido de la pandemia como hoy en día.

Cabe apuntar que se trata de datos especialmente sensibles pues, al ser información relacionada con la esfera íntima del ciudadano, en concreto su estado de salud, necesitan de una regulación diferenciada respecto a otro tipo de datos personales. Así lo expone el criterio jurisprudencial: *"la información relativa a la salud física o psíquica de una persona, en suma, es no sólo una información íntima (SSTC 202/1994, de 4 de julio, FJ 2; y 62/2008, de 26 de mayo, FJ 2), sino además especialmente sensible desde este punto de vista y por tanto digna de especial protección desde la garantía del derecho a la intimidad"* (STC 70/2009)[48]. Asimismo, en el ordenamiento jurídico español

[48] Tribunal Constitucional (Pleno). Sentencia núm. 70/2009, de 23 de marzo de 2009. ECLI:ES:TC:2009:70

existe mención expresa a los datos especialmente sensibles, tanto en el art. 9 de la LOPDGDD (recogidos como "categorías especiales de datos"), como en el RDPD.

Las autoridades se pronunciaron al respecto afirmando que "*el RGPD y demás normativa no debe obstaculizar las medidas que hayan de tomarse en la lucha contra la pandemia"* (CEPD, 2020).

Por lo tanto, sabiendo que se permite el tratamiento de datos relacionados con la salud de las personas, sin consentimiento del interesado y por razones de interés público (como es la lucha contra cualquier epidemia o pandemia), y que así ha sucedido en el marco de la COVID-19, no es extraño preguntarse ahora sobre su alcance en las relaciones laborales. Numerosos empresarios se han visto en la obligación de adoptar medidas urgentes y tratar con datos íntimos cuestionándose a su vez la legalidad de dichas actuaciones. Resulta interesante atajar este punto y analizar al detalle las posibles respuestas a aquellas cuestiones que tanto la AEPD como los despachos de abogados están recibiendo diariamente.

¿A qué datos de los trabajadores puede acceder el empleador durante la COVID-19? ¿Cuál es la base jurídica y su finalidad?

A diferencia de casos pre-pandémicos en los que el empresario no tenía el derecho a conocer el motivo de enfermedad o baja de uno de sus empleados en caso de que estos no se lo proporcionaran, con la llegada del COVID-19, el empresario podrá acceder a los datos de salud del empleado que tengan relación con los síntomas, el contagio o la evolución de la enfermedad.

Para ello, podrá preguntar tanto al empleado en cuestión como al resto del equipo y, se trata de un mínimo de datos necesarios, ni excesivos ni detallados, que tienen por objeto ayudar al empresario a planificar una respuesta lo más rápida posible ante tal contingencia. Tal y como defiende la AEPD, en caso de que exceda en sus funciones y el empresario realice cuestionarios de salud extensos y detallado o que incluyan preguntas que nada tengan que ver con lo expuesto, resultaría contrario al principio de minimización de datos (AEPD, 2020).

Además, puede acceder a datos sobre la localización de los empleados dentro de la empresa, posibles contactos o viajes realizados. Todo ello, con el objeto de llevar a cabo un rastreo o exploración interna para la no propagación del virus y el mantenimiento de la extrema precaución.

No obstante, hoy día la cuestión más controvertida en el ámbito laboral como consecuencia de la pandemia es, si de la misma manera, el empresario podrá acceder a la localización de los trabajadores cuando estos se encuentren fuera de su jornada laboral. Según la literalidad del art. 6.1 a) RGPD, esto solo podrá ser posible en caso de que existiera consentimiento expreso por parte de los empleados. Sin embargo, la jurisprudencia completa lo dispuesto anteriormente legitimando así al empresario a conocer determinados datos de un trabajador pese a estar este fuera de su jornada laboral y no haber dado consentimiento expreso (STS 766/2020)[49]. Para ello, se requiere de la concurrencia de una serie de circunstancias que sí se daban en el caso objeto de estudio de la presente sentencia.

Entre los hechos que se han analizar, cabe destacar los siguientes: la titularidad del dispositivo que sirve como objeto de geolocalización, conocimiento del trabajador del geolocalizador, el fin último del dispositivo y la intencionalidad en el uso del mismo por parte del empleado.

El sustento jurídico del tratamiento reside tanto en el artículo 9.2.b) del RGPD[50], como en el art. 6.1.c)[51] de la misma norma. Todo lo anterior exhibe que tanto el cumplimiento de una obligación legal en el ámbito laboral como la protección de intereses vitales, públicos o legítimos son causa justificada para el tratamiento. Por otra parte, lo dispuesto en la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales (en adelante, LPRL) también sirve como base jurídica pues en su artículo 14 fija lo siguiente: *"el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo", "el empresario realizará (…) cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores".*

Por lo expuesto, se concluye que la finalidad que se persigue mediante el tratamiento de datos reside en dos aspectos principales. En primer lugar, vigilar y proteger

---

[49] Tribunal Supremo. Sentencia núm. 766/2020, de 15 de septiembre de 2020. Rec. 528/2018. ECLI:ES:TS:2020:3017

[50] Art. 9.2.b) RGPD: *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".*

[51] Art. 6.1.C) RGPD: *"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento".*

la salud de los trabajadores y de la población en general y, en segundo lugar, diseñar planes de contingencia que sean necesarios, o que hayan sido previstos por las autoridades sanitarias (AEPD, 2020).

Por lo tanto, parece evidente que los deberes de diligencia y buena fe empresarial inherentes a la condición de empresario pasan (a la vista de la literalidad de la norma) por garantizar la seguridad y la salud de los trabajadores a través, en este caso, de medidas de vigilancia y control para evitar contagios masivos dada la transmisibilidad de la enfermedad de la COVID-19. Se trata en definitiva de la ponderación por parte del empresario empleador de dos derechos fundamentales, con prevalencia en este caso y dada su especial importancia en estos tiempos del derecho a la salud.

¿Es necesario el consentimiento del empleado para vigilar la salud?

El artículo 22.1 de la LPRL dispone que: *"El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo.*

Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo".

Por lo tanto, considerando el principio general para la vigilancia de salud, esta medida solo podría llevarse a cabo si existiera consentimiento por parte del trabajador y excepcionalmente si se trata de un supuesto recogido en el art. 22.1 LPRL segundo párrafo.

¿Cuál es la obligación del trabajador con síntomas, en cuarentena preventiva o infectada por COVID-19 de informar al empresario?

El trabajador que dentro de la plantilla se encuentre con síntomas de COVID-19, afectado por el mismo o incluso en cuarentena preventiva, tiene la obligación de informar a la empresa de ese extremo pues debe velar por su propia seguridad y salud, y por la de aquellas otras personas a las que pueda afectar su actividad profesional, así lo establece el art. 29.4.4º de la LPRL[52] que versa sobre las obligaciones de los trabajadores en materia de prevención de riesgos.

Como consecuencia del incumplimiento de dichas obligaciones, el empleado incurrirá en "incumplimiento laboral muy grave" recogido en el Capítulo IV, art. 58 del ET. Por consiguiente, el empresario podrá imponer sanciones que variarán en función de lo estipulado en el convenio colectivo, la intencionalidad de la parte actora o la gravedad de las actuaciones. Entre dichas sanciones se encuentra la posibilidad de proceder al despido disciplinario del acusado, no obstante, se ha de aportar prueba suficiente que acredite visiblemente la infracción.

¿Puede la empresa comunicar a otros empleados que un trabajador determinado tiene COVID-19?

En condiciones normales, la empresa no podrá trasladar al resto de la plantilla la infección por COVID-19 de un trabajador salvo que sea estrictamente necesario.

¿Puede la empresa tratar los datos de los visitantes a un centro de trabajo?

Siempre y cuando se tenga por objeto la protección de la seguridad y la salud de los trabajadores (como veníamos exponiendo en apartados anteriores), el empresario podrá escudar el tratamiento de datos de visitantes.

[52] Art. 29.2. LPRL: "*Los trabajadores, con arreglo a su formación y siguiendo las instrucciones del empresario, deberán en particular: 4º. Informar de inmediato a su superior jerárquico directo, y a los trabajadores designados para realizar actividades de protección y de prevención o, en su caso, al servicio de prevención, acerca de cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores."*

¿Puede utilizar la empresa cualquier tecnología que considere oportuna para identificar casos de COVID-19?

La empresa puede someter al trabajador a una "*vigilancia regular*" basada en reconocimientos médicos y otras pruebas que *"proporcionales al riesgo, causen las menores molestias al trabajador"* (Mendoza, 2007).

¿Se puede tomar la temperatura a los trabajadores? Y, ¿encomendar a un empleado o persona de seguridad que mida la temperatura de los empleados?

Si la finalidad del tratamiento de este tipo de datos de salud se limita a la detención de posibles contagios, se lleva a cabo con equipos homologados y por el personal de prevención o personal sanitario, podrán tomar la temperatura a los empleados.

En relación con lo anterior, esta práctica no podrá ser realizada por cualquier miembro de la plantilla. Atendiendo al Art 22.6 LPRL: "*Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada".* De manera análoga, estos profesionales reservarán para si mismos esta información.

La AEPD manifestó su intranquilidad sobre el descontrol que sobrevenía en las empresas durante la pandemia en relación con la medición de temperatura a empleados y visitantes pues, aseguraban que se estaba practicando sin haber consultado primeramente a las autoridades sanitarias expertas en el asunto (AEPD, 2020).

Si bien es una realidad que se trata de una práctica muy común en las empresas durante la pandemia, es importante atender a la importancia del cumplimiento de todas exigencias establecidas en la ley. Por ejemplo, el hecho encomendar la tarea de medición de temperatura a un empleado o persona de seguridad (y, por tanto, no expertos) daría lugar a importantes consecuencias. Entre ellas, por un lado, la empresa se enfrentaría a una infracción de confidencialidad de datos personales y por otro, incurriría en un riesgo para la salud.

Adicionalmente, ante la imposibilidad de acudir de manera presencial a las oficinas, prestar servicios bajo la modalidad de teletrabajo se convirtió en el modelo predominante. Algunas de las empresas venían incluyendo este tipo de prestación de servicios en sus regímenes[53], sin embargo, la gran mayoría se vieron expuestos ante un

[53] Véase, IBM, Yahoo, Bank of America y Best Buy (Villadiego, 2020).

escenario completamente desconocido y no merecedor de minusvaloración. Ello se debe a los abundantes factores a tener en cuenta en materia de protección de datos cuando se trata de teletrabajo y ciberseguridad.

¿Qué papel tiene el empresario en relación con el teletrabajo?

La empresa debe adoptar medidas técnicas y organizativas[54] para garantizar el tratamiento lícito de los datos de carácter personal que lleven a cabo sus trabajadores fuera del entorno físico laboral[55] (art. 32 RGPD), entre las que cabe destacar:

- Garantizar que todos los dispositivos que vayan a manejar los empleados cumplan con medidas de seguridad.

- Asegurarse que las redes de internet que vayan a utilizar los trabajadores en sus comunicaciones con la empresa, con clientes o terceros sean seguras.

- Concienciar al personal de la importancia del tratamiento de datos, para evitar que estos puedan compartirse con terceros o puedan ser eliminados sin autorización. Todo el personal debe notificar cualquier incidencia que pueda producirse en el tratamiento de los mismos.

- Advertir al personal de que, en ningún caso, pueden deshacerse de documentos que contengan datos personales si no es de un modo seguro (nunca en las papeleras o "cubos de basura" sino mediante destructores de papel)

[54] Que, a su vez podrán ser: preventivas o reactivas.
[55] Véase, el análisis de la AEPD: *"no es posible asegurar el derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales".*

6. NECESIDAD DE INFORME PERICIAL EN JUICIOS PARA LA VALIDEZ DE LAS PRUEBAS

El objeto de la prueba no es otro que confirmar testimonios que apoyen la postura en un conflicto entre partes, persiguiendo de esta manera convencer al juez (de Rey Rodríguez y Sebastián, 2006). Es indiscutible que esta afirmación es extrapolable a todas las ramas del derecho pues se trata de fórmulas que sirven para acreditar la veracidad o falsedad de una versión cualquiera, independientemente de si nos encontramos ante la jurisdicción civil, penal, contencioso-administrativa o social.

Adicionalmente, el artículo 85.6 de la Ley Reguladora de la Jurisdicción Social (en adelante, LRJS) establece la obligación de fijar los hechos sobre los que exista conformidad o disconformidad de los litigantes. Consecuentemente, en virtud del art. 281.3 LEC, las partes prepararán su defensa y oportuna prueba respecto de aquellas cuestiones sobre las que conste discrepancia, estando así libres de prueba aquellos asuntos sin disputa. Así mismo, y en virtud de lo establecido en el art. 281.2 LEC *"también serán objeto de prueba la costumbre y el derecho extranjero".* Todas las pruebas que se aporten en el juicio han de ser conforme a lo que entiende la LEC como "medio de prueba" en su art. 299[56].

En virtud de lo señalado en el art. 90.1 de la LRJS[57], la admisibilidad de la prueba queda supeditada únicamente a que estas se presenten a tiempo y a que se justifique la utilidad y pertinencia de las diligencias necesitadas de prueba. Habida cuenta lo anterior, no se debe pasar por alto que, en ningún caso resultarán de admisión aquellas pruebas que transgredan derechos fundamentales y de esta manera lo establece el art. 11 LOPJ. Por

[56] Art. 299 LEC. Medios de prueba:
1. Los medios de prueba de que se podrá hacer uso en juicio son:
1. º Interrogatorio de las partes.
2. º Documentos públicos.
3. º Documentos privados.
4. º Dictamen de peritos.
5. º Reconocimiento judicial.
6. º Interrogatorio de testigos.
2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.
3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.

[57] Art. 90.1 LRJS *"Las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba"*

ello, a continuación, se analizará qué líneas se han de seguir para la inclusión de datos personales en la aportación de pruebas pues es la materia objeto de estudio del presente trabajo.

El art. 18.3 CE que asegura que *"se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"*, y resulta necesario analizar dicho artículo en el contexto de lo establecido en el art. 90.4. LRJS que establece que *"cuando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través de juicio de proporcionalidad y con el mínimo sacrificio, determinando las condiciones de acceso, garantías de conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso*". Es importante tener en cuenta estos artículos y considerar tanto la importancia del respeto a los derechos fundamentales, como los pasos a seguir durante la aportación de pruebas que recaigan sobre datos personales en un procedimiento de cualquier jurisdicción.

El TS, en el contexto de un presunto delito contra la salud pública, anuló el valor probatorio de unas intervenciones telefónicas y estimó el recurso de los presuntos autores, ya que consideraba que vulneraban el derecho fundamental a la intimidad (STS 740/1997)[58]. Argumentó la sala que dichas pruebas no cumplían con unos principios básicos pues, ni estaban fundadas (no había motivación ni proporcionalidad), ni había habido control judicial suficiente, entre otras cosas. Con todo ello, la aceptación de las intervenciones telefónicas como prueba hubiera supuesto en este caso, una clara intromisión a la intimidad de los individuos.

Cabe destacar que desde la llegada de internet hace más de 60 años, la comunicación ha cambiado drásticamente y, como se ha adelantado anteriormente, es extrapolable al ámbito laboral. La mayor parte de las conversaciones empresario-trabajador se llevan a cabo a través de correo electrónico, WhatsApp u otro tipo de redes sociales. En el supuesto de que sobrevenga conflicto y posterior juicio entre ambas partes, es frecuente

[58] Tribunal Supremo. Sentencia núm. 740/1997, de 26 de mayo de 1997. Rec. 158/1996

que se aporten pruebas de conversaciones mantenidas a través de este tipo de plataformas lo que puede tener efecto directo sobre el art. 18.3 CE.

Para solucionar el supuesto anterior, se acude a informes periciales que se encarguen de dotar de validez y eficacia procesal a la prueba objeto de controversia. De esta manera, se aseguran que lo aportado cuente con las máximas garantías y que el Juez adquiera un dictamen sobre conocimientos técnicos que no posee. El trabajo de estos profesionales es imprescindible pues "*en materia de prueba electrónica lo esencial es invisible para nuestros ojos*" (Leon y Valero, 2016).

En este sentido, el TS sienta lo siguiente: "*Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido"* (STS 300/2015)[59]. Dicho argumento confirma la importancia de la figura de un experto y su oportuno dictamen pues, de lo contrario, nadie nos aseguraría que no se quebrantaran otros derechos fundamentales a la hora de pruebas en procesos judiciales.

[59] Tribunal Supremo. Sentencia núm. 300/2015, de 19 de mayo de 2015. Rec. 2387/2014. ECLI:ES:TS:2015:2047

7. CONCLUSIONES

Como se ha ido exponiendo a lo largo del trabajo, la ausencia de una clara delimitación conceptual de los derechos correspondientes a la esfera privada de la persona genera en la sociedad una innegable inseguridad jurídica. Si bien es cierto, conviene recordar que se trata de derechos inherentes al ser humano y que, por tanto, le acompañan en los diferentes ámbitos de su vida, entre los que se incluye la prestación de servicios.

Estos derechos a la intimidad, privacidad y protección de datos de las personas en el seno de las relaciones laborales entran en conflicto con los poderes del empresario. A lo largo de este trabajo se han detallado los límites, así como los principios básicos que el empresario ha de respetar a la hora de ejercer sus poderes. No obstante, en la presente sección del estudio me gustaría realizar una aproximación subjetiva sobre la rigurosidad de la normativa laboral española en lo referente al poder del empresario y su influencia en la economía en general pues, en ocasiones la realidad se aleja visiblemente de las exigencias normativas.

Mientras que unos teóricos piensan que el empresario ha de tener un control mínimo durante el desarrollo de la prestación de servicios de los trabajadores, otros piensan que es necesario que este goce bien de un mayor número de facultades, bien de una menor limitación de estas.

Como se ha visto, tanto en la legislación estudiada como en los casos analizados se pone de manifiesto cómo el ejercicio de poder del empresario se ve muy limitado y sumamente restringido pues, a juicio de esta parte, los límites impuestos a la figura del empresario son en la realidad excesivos. Uno de los supuestos ejemplo de lo mencionado es el Caso López Ribalda (citado a lo largo del trabajo).

No obstante, en caso de conflicto se ha de analizar individualmente las circunstancias y, en ultima instancia, serán los tribunales quienes conozcan el caso. Como en todo proceso, ambas partes aportarán las pruebas oportunas y el tribunal sentenciará imparcialmente y conforme a lo establecido en la norma.

Pese a la complejidad que concierne la materia, se ha de tener en consideración que las empresas son el motor de la economía en el país y que las autoridades han de facilitar la contratación laboral con condiciones lo más favorable posible para ambas partes de manera que nadie resulte desprotegido.

Si bien es cierto, la realidad es cambiante y el Derecho Laboral evoluciona de su mano. Las empresas, los trabajadores y los tribunales se ven obligados a mantenerse actualizados de la última tecnología y su influencia en las relaciones laborales. Uno de los mayores ejemplos de esta realidad es lo ocurrido con la llegada de la pandemia en 2020, contingencia ante la cual muchos de los empresarios han tenido que adaptarse y cambiar radicalmente su estructura empresarial (implantación de medios tecnológicos innovadores y desconocidos, teletrabajo, sistemas de geolocalización, control de la salud…).

8. NORMATIVA Y JURISPRUDENCIA REFERENCIADA

- **Normativa**

Carta de los Derechos Fundamentales de la Unión Europea. (DOUE núm. 83, de 30 de marzo de 2010)

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

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. (BOE núm. 243, de 10 de octubre de 1979).

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (BOE núm. 7, de 8 de enero de 2000).

Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales. (BOE núm. 269, de 10 de octubre de 1995)

Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social. (BOE núm. 245 de 11 de octubre de 2011).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. (BOE núm. 157, de 2 de julio de 1985).

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

Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. (BOE núm. 86, de 28 de marzo de 2020).

Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. (BOE núm. 131, de 2 de junio 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)

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) (DOUE núm. 119, de 4 de mayo de 2016).

Tratado de la Unión Europea y Tratado de Funcionamiento de la Unión Europea. Versiones consolidadas. (DOUE. núm. 83, de 30 de marzo de 2010).

- **Jurisprudencia**

Tribunal Europeo de Derechos Humanos. Sentencia de 5 de septiembre de 2017. Caso Bârbulescu contra Rumanía. ECLI:CE:ECHR:2017:0905JUD006149608

Tribunal Europeo de Derechos Humanos. Sentencia de 17 de octubre de 2019. Caso López Ribalda II contra España. ECLI:CE:ECHR:2019:1017JUD000187413

Tribunal Constitucional (Pleno). Sentencia núm. 101/1983, de 18 de noviembre de 1983. ECLI:ES:TC:1983:101

Tribunal Constitucional (Pleno). Sentencia núm. 88/1985, de 19 de julio de 1985. ECLI:ES:TC:1985:88

Tribunal Constitucional (Pleno). Sentencia núm. 20/1992, de 14 de febrero de 1992. ECLI:ES:TC:1992:20

Tribunal Constitucional (Pleno). Sentencia núm. 50/1995, de 31 de marzo de 1995. ECLI:ES:TC:1995:50

Tribunal Constitucional (Pleno). Sentencia núm. 292/2000, de 30 de noviembre de 2000. ECLI:ES:TC:2000:292

Tribunal Constitucional (Pleno). Sentencia núm. 70/2009, de 23 de marzo de 2009. ECLI:ES:TC:2009:70

Tribunal Constitucional (Pleno). Sentencia núm. 170/2013, de 7 de octubre de 2013. ECLI:ES:TC:2013:170

Tribunal Constitucional (Pleno). Sentencia núm. 148/2021, de 14 de julio de 2021. ECLI:ES:TC:2021:148

Tribunal Supremo. Sentencia núm. 740/1997, de 26 de mayo de 1997. Rec. 158/1996

Tribunal Supremo. Sentencia de 26 de septiembre de 2007. Rec. 966/2006. ECLI:ES:TS:2007:6128

Tribunal Supremo. Sentencia de 6 de octubre de 2011. Rec. 4053/2010. ECLI:ES:TS:2011:8876

Tribunal Supremo. Sentencia núm. 678/2014, de 20 de noviembre de 2014. Rec. 3402/2012. Rec. 3402/2012. ECLI:ES:TS:2014:5215

Tribunal Supremo. Sentencia núm. 97/2015, de 24 de febrero de 2015. Rec. 1774/2014. ECLI:ES:TS:2015:823

Tribunal Supremo. Sentencia núm. 300/2015, de 19 de mayo de 2015. Rec. 2387/2014. ECLI:ES:TS:2015:2047

Tribunal Supremo. Sentencia núm. 53/2015, de 23 de septiembre de 2015. Rec. 648/2015. ECLI:ES:2015:3874

Tribunal Supremo. Sentencia núm. 119/2018, de 8 de febrero de 2018. Rec.1121/2015. ECLI:ES:TS:2018:594

Tribunal Supremo. Sentencia núm. 1033/2020, de 25 de noviembre de 2020. Rec. 39/2019. ECLI:ES:TS:2020:4187

Tribunal Supremo. Sentencia núm. 766/2020, de 15 de septiembre de 2020. Rec. 528/2018. ECLI:ES:TS:2020:3017

Tribunal Superior de Justicia de Valencia. Sentencia núm. 2716/2021, de 5 de octubre de 2010. Rec. 2195/2010. ECLI:ES:TSJCV:2010:7242

Tribunal Superior de Justicia de Andalucía, Sevilla. Sentencia núm. 905/2019, de 28 de marzo de 2019. Rec. 744/2018. ECLI:ES:TSJAND:2019:1355

Tribunal Superior de Justicia de Andalucía, Málaga. Sentencia núm. 566/2021, de 24 de marzo de 2021. Rec. 316/2021. ECLI:ES:TSJAND:2021:5399

Tribunal Superior de Justicia de la Región de Murcia. Sentencia núm. 82/2022, de 26 de enero de 2022. Rec. 754/2021. ECLI:ES:TSJMU:2022:35

Jugado de lo Social núm. 26 de Barcelona. Sentencia de 18 de noviembre de 2021. Procedimiento núm. 177/2020. ECLI:ES:JSO:2021:7119

9. BIBLIOGRAFÍA

Abellán, I. M. (2003). Sinopsis artículo 53. Constitución Española. *Congreso de los Diputados.*https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=53&tipo=2

Agencia Española de Protección de Datos (2020). Informe del Gabinete Jurídico (Nro. 0017/2020). Gobierno de España. https://www.aepd.es/es/documento/2020-0017.pdf

Agencia Española de Protección de Datos. (2020, 30 de Abril). Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos [comunicado de prensa prensa]. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

Alexy, R. (2011). Los derechos fundamentales y el principio de proporcionalidad. *Revista española de derecho constitucional*, 11-29.

Álvarez, J. L. D. (2021). La tutela jurídica de la protección de datos de carácter personal en el horizonte post COVID-19. Nuevos compromisos para las Administraciones públicas. *Revista Aranzadi de derecho y nuevas tecnologías*, (55), 6.

Carmona Cuenca, E. (2004). El principio de igualdad material en la Constitución Europea.

Cazurro Barahona, V. (2020). Antecedentes y fundamentos del Derecho a la protección de datos. Antecedentes y fundamentos del Derecho a la protección de datos, 1-152.

Comité Europeo de Protección de Datos (2020). Declaración sobre el tratamiento de datos personales en el contexto de la reapertura de las fronteras tras el brote de la COVID-19 del 16 de junio de 2020.

Cotteleer, M. y Snideran, B. (2018). *Forces of change: Industry 4.0. Deloitte Insights*. https://www2.deloitte.com/content/dam/Deloitte/es/Documents/manufacturing/Deloitte-ES-manufacturing-industria-4.0.pdf

Covid-19: Un antes y después en el teletrabajo y sus implicaciones en ciberseguridad. (2020). Obtenido de: https://forbes.co/2020/08/03/red-forbes/covid-19-un-antes-y-despues-en-el-teletrabajo-y-sus-implicaciones-en-ciberseguridad/

Crespo, M. J. R. (2018). La Necesaria observancia de los derechos fundamentales en las relaciones laborales como límite inexcusable del poder de dirección empresarial. *IUSLabor. Revista d'anàlisi de Dret del Treball*, (2), 173-185.

de Marcos, L. D. F. (2021). Accountability en mi entidad: qué, quién, cómo, cuándo y por qué. *Actualidad administrativa*, (9), 5.del Pozo Benítez, P., & Mañá, J. P. (1996). El derecho de acceso y distribución de información por vía telemática como derecho fundamental. *Informática y derecho: Revista iberoamericana de derecho informático*, (12), 1393-1400.

De Mendizábal, P. Próximo reto de la privacidad y protección de datos: el metaverso. *Legaltoday*. http://www.laleyaldia.cl/?p=14835

del Rey Rodríguez, I. G., & Sebastián, P. M. (2006). La prueba en el proceso laboral: objeto, carga y posibilidades de impugnación. *Aranzadi social*, (5), 777-812.

Del Rosal, P. (30 de mayo de 2019). La empresa no puede acceder al historial de navegación del ordenador de los empleados. *El País*. https://cincodias.elpais.com/cincodias/2019/05/30/legal/1559196028_877451.html

Delgado Jiménez, A. F. (2020). La privacidad del trabajador y el control tecnológico de la actividad laboral.

Esteban, P. (4 de abril de 2022). Es ilegal registrar los ordenadores en el trabajo sin previo aviso. *El País*. https://cincodias.elpais.com/cincodias/2022/04/01/legal/1648795074_620659.html

Esteban, P. (5 de marzo de 2022). Un derecho por escribir en el metaverso. *El País*. https://elpais.com/economia/negocios/2022-03-05/un-derecho-por-escribir-en-el-metaverso.html

Fabregat Monfort, G. (2016). El poder de dirección del empleador: poder de dirección stricto sensu, ius variandi empresarial y poder de control, vigilancia y sanción al trabajador. *Nuevas perspectivas del poder de dirección y control del empleador*, 17-19.

Fabregat Monfort, G. (2016). Manifestaciones concretas del poder de control del empleador en el desarrollo de la relación laboral. *Nuevas perspectivas del poder de dirección y control del empleador*, 39-91.

Fraguío, P. D. (2018). La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento

General de Protección de Datos). *REDE. Revista española de derecho europeo*, (68), 113-148.

Garcia-Poveda, C. (2018). *La regulación de los ficheros de solvencia patrimonial y de crédito en el nuevo RGPD: La causa de legitimidad del tratamiento* (Master's thesis).

Garriga Domínguez, A. (2016). Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. *Nuevos retos para la protección de datos personales*, 176-177.

López, M. C. P. (2003). Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos. In El modelo social en la Constitución española de 1978 (pp. 229-248). Subdirección General de Publicaciones.

Maroto, J. M. D. (2018). *Datos personales biométricos dactiloscópicos y derechos fundamentales: nuevos retos para el legislador* (Doctoral dissertation, UNED. Universidad Nacional de Educación a Distancia (España)).

Martínez de Pisón Cavero, J. M. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. *Anuario de filosofía del derecho*, 409-430.

Martínez, J. A. G. (2021). La videovigilancia empresarial en la industria 4.0: la salvaguarda de la intimidad informática del trabajador. Revista Aranzadi Doctrinal, (10), 4.

Martínez, J. I., & Zúñiga Urbina, F. (2011). El principio de razonabilidad en la jurisprudencia del Tribunal Constitucional. *Estudios constitucionales*, *9*(1), 199-226.

Martínez, R. M. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, (5), 4.

Mendoza Navas, N. (2007). Prevención de riesgos laborales: la regulación convencional. *Albacete: Bomarzo (versión on line)*.

Montoro, L. G. (2015). Wearables: qué son, cómo funcionan y que peligros entrañan para nuestra privacidad. *Centro de Estudios de Consumo, Universidad de Castilla La Mancha*.

Navarro, A. V. S. (2020). Vídeo-comentario a la STS 119/2018, de 8 febrero (RJ 2018, 666). *Examen del correo electrónico del trabajador acordado tras el hallazgo casual de*

fotocopias de las transferencias bancarias efectuadas por un proveedor en favor del trabajador: realización de prueba pericial limitada a los correos relativos a las transferencias, sin presencia de notario o representación de los trabajadores u otro trabajador o el interesado [Video]. *Aranzadi social.* https://webcastlive.es/aranzadi/actualizacion-profesional/2018.htm?id=STS-119-2018_08-02-2018_RJ-2018-666

Nisa Ávila, J. A. (8 de octubre de 2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. *"La Inteligencia artificial, IOT y data mining: una nueva perspectiva jurídica de la teoría del mosaico"*. El Derecho. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

Oliva Leon, R., & Valero Barcelo, S. (2016). La prueba electrónica: validez y eficacia procesal: ¿En qué consiste la prueba electrónica? ¿Qué elementos debe reunir para que sea válida y eficaz en el proceso? ¿Se puede manipular?

Olivares, B. D. O. (2021). ¿Hacia una conservación ilimitada de los datos personales por parte de la Administración tributaria? *Quincena fiscal*, (4), 25-51.

Olivares, B. D. O. (2021). El tratamiento lícito de la información y las limitaciones del derecho a la protección de datos en el ordenamiento tributario. *La protección de los derechos fundamentales en el ámbito tributario* (pp. 157-188). Wolters Kluwer España.

Orrico, F. J. F. (2019). Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre. Nueva revista española de derecho del trabajo, (222), 31-76.

Palomar, A y Fuertes, F. J. (2022). Práctico de protección de datos de carácter personal. https://app.vlex.com/#search/jurisdiction:ES/delegado+de+proteccion+de+datos/WW/vid/716170277

Puig, P. M. T. (2001). Valores y principios constitucionales. *Parlamento y Constitucion. Anuario*, (5), 129-143.

Rojo Torrecilla, E. El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales. *Blog personal del autor*, *20*.

Tillería, S. H. (2019). Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II. *IUSLabor. Revista d'anàlisi de Dret del Treball*, (3), 55-80.

Timón Herrero, M. Protección de datos de carácter personal y crisis sanitaria (Covid-19). [Entrada de blog]. *ElDerecho.com*.

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. Isegoría Revista de Filosofía Moral y Política, (57), 533-552.

Trías, R., RUIZ, E. Y. A., & Angeles, M. (2013). Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española. In *Conferencia Trilateral Italia/Portugal/España Roma* (Vol. 24).

Ugarte Cataldo, J. L. (2011). Privacidad, trabajo y derechos fundamentales. *Estudios constitucionales*, *9*(1), 13-36.

Villadiego, R. (3 de agosto de 2020). Covid-19: Un antes y después en el teletrabajo y sus implicaciones en ciberseguridad. *Forbes*. https://forbes.co/2020/08/03/red-forbes/covid-19-un-antes-y-despues-en-el-teletrabajo-y-sus-implicaciones-en-ciberseguridad/