universidad de león

GRADO EN RELACIONES LABORALES

Y RECURSOS HUMANOS
FACULTAD DE CIENCIAS DEL TRABAJO

UNIVERSIDAD DE LEÓN

CURSO 2019/2020

SISTEMAS TECNOLÓGICOS DE CONTROL,

UN CONFLICTO DE INTERESES.

TECHNOLOGICAL CONTROL SYSTEMS,

A CONFLICT OF INTERESTS.

Realizado por el Alumno D. ALFONSO HERRERO SANZ

Tutorizado por el Profesor D. RODRIGO TASCÓN LÓPEZ

ÍNDICE

1 RESUMEN

Resumen:

El presente trabajo muestra el grado de influencia de las nuevas tecnologías de la información y comunicación sobre los actores principales de una relación laboral. A través de un leve acercamiento a la normativa sobre la protección de datos de carácter personal, fundamental para salvaguardar y proteger derechos fundamentales, y a la evolución de los tribunales en sus pronunciamientos, se persigue encontrar la fina línea que separa la libertad empresarial para ejercer su facultad de vigilancia y control de la vulneración de derechos constitucionalmente reconocidos, y de esta forma, intentar encontrar el punto de equilibrio en este juego de intereses.

Palabras clave: Reglamento (UE) 2016/679, trabajador, sentencia, información previa, TICs.

Abstract:

This work shows the degree of influence of the new information and comunication technologies on the main actors in the contex of an employment relationship.

Through slight approaching to regulations on personal data protección, very important in safeguarding and protect fundamental rights, and the courts development in its pronuncement of judgement. We pursue to find the fine line between the entrepreneurial freedom in order to exert it right of monitoring and control of the violation of the constitucional rights and in this way, to try to find a balance in this game of interests.

Key words: Regulation (UE) 2016/679, worker, judgement, previous information, ICT4D.

2 OBJETO DEL TRABAJO

Consecuencia de la irrupción y consolidación de las nuevas tecnologías de la información y comunicación en la sociedad, y en particular, en las organizaciones empresariales, surgen nuevas formas de vigilancia y control sobre el trabajador en el ámbito laboral, y con ellas, nuevos riesgos de colisión entre derechos fundamentales del trabajador y las mencionadas modalidades tecnológicas de vigilancia y control.

Esta problemática adquiere un mayor interés tras las recientes normativas aprobadas sobre protección de datos de carácter personal, el Reglamento (UE) 2016/679, de 27 de abril, en el marco de la Unión Europea, y la Ley Orgánica 3/2018, de 5 de diciembre, en el ámbito nacional.

Este trabajo presenta una noción general, a través de la normativa vigente en protección de datos personales y los pronunciamientos de los tribunales, de los límites existentes en la facultad del empresario de vigilancia y control mediante las nuevas tecnologías, y los requisitos, que han sido y son estudiados y señalados, por el Reglamento (UE) 2016/679 y los tribunales, en relación al acceso y tratamiento de los datos de carácter personal de los trabajadores, y en particular, los especialmente sensibles.

Por lo tanto, para poder analizar y comprender la realidad de las relaciones laborales, tendremos que conocer la evolución en los pronunciamientos de los tribunales, los requisitos y límites que demanda la normativa o, la importancia que tienen los convenios colectivos y políticas de empresa en las organizaciones empresariales en este sentido.

Por tanto, el objeto de este trabajo consiste en que se comprendan, mediante la normativa vigente en protección de datos personales y la jurisprudencia, donde está el límite de vigilancia y control tecnológico del empresario.

3 METODOLOGÍA

La metodología utilizada para la elaboración del presente trabajo ha sido, prácticamente en su totalidad, jurídica.

En primer lugar, han sido leídos dos trabajos científicos y una obra monográfica relacionadas con el tema a tratar, así como proceder a la documentación y análisis de la normativa vigente que podía ser de interés. A partir de la información recabada, y sirviendo como guía determinadas palabras clave utilizadas en la distinta bibliografía consultada, ha sido realizado un índice provisional.

Posteriormente, una vez realizado el índice provisional, y usando éste como apoyo, han sido buscadas obras monográficas y secciones de libros a través del catálogo de la biblioteca de la Universidad de León. Por otro lado, han sido objeto de búsqueda: Artículos doctrinales, comentarios prácticos, documentos de interés y jurisprudencia, siempre a través de la plataforma digital Aranzadi Instituciones.

El día 15 de marzo fue decretado el Estado de Alarma, por ello, y debido a las circunstancias tan extraordinarias que nos ha tocado sufrir, he dispuesto solamente de una obra monográfica, centrando el presente trabajo en artículos doctrinales de revistas jurídicas y en la jurisprudencia facilitada por la base de datos Aranzadi Instituciones.

Aprovechando la emergencia sanitaria que hemos y estamos pasando, he creído de interés investigar y sintetizar información que relacione el COVID-19 y las organizaciones empresariales. La manera de proceder a la documentación, para tratar dicho tema, ha sido mediante artículos doctrinales y el correspondiente informe emitido al respecto por la Agencia Española de Protección de Datos.

Finalmente, y atendiendo a los objetivos anteriormente descritos, ha sido relacionada la información recabada, mediante las fuentes ya mencionadas, para poder comprenderla y posteriormente plasmarla en este trabajo.

4 INTRODUCCIÓN

Nos hayamos en un momento de nuestra historia, en el cual, es indudable la presencia y el grado de condicionamiento que las nuevas tecnologías de la información y comunicación ejercen sobre la sociedad y por supuesto, sobre las organizaciones empresariales y las relaciones laborales con sus trabajadores.

Consecuencia de las nuevas tecnologías, se han abierto los mercados comerciales y hay una mayor competitividad, lo cual lleva, por parte de las empresas, a una búsqueda constante de la optimización de recursos y reducción de costes, con el claro objetivo de mejorar los procesos productivos y así aumentar la productividad.

El problema se presenta cuando observamos lo que supone esto para los trabajadores. Las empresas necesitarán una menor mano de obra debido a la aparición de las nuevas tecnologías, búsqueda constante de optimización de recursos y reducción de costes, por lo que nos encontramos ante una clase trabajadora que acepta condiciones precarias de trabajo y que está más sometida al empleador por la necesidad de mantener el puesto de trabajo, puesto que existe miedo e incertidumbre a no acceder de nuevo al mercado laboral (Rodriguez Escanciano, 2015).

Esta situación de desigualdad jerárquica creciente, y en muchas ocasiones de subordinación, entre el empresario y el trabajador, puede provocar un aumento en el poder de vigilancia y control del empleador, suponiendo en cierto modo, un control impersonal y continuo sobre el propio trabajador, puesto que la mejora tecnológica y la escasez de ofertas de empleo se lo permiten.

En este contexto tan poco esperanzador, de optimización al máximo de los recursos, control impersonal sobre el trabajador y revolución tecnológica, cabe preguntarse en qué medida podrá utilizar el trabajador los medios informáticos, propiedad de la empresa, y hasta qué punto será posible, sin vulnerar derechos fundamentales, la vigilancia y control empresarial mediante las herramientas tecnológicas que estén a su alcance, las cuales, van a permitir controlar milimétricamente los pasos que dé el trabajador en el centro de trabajo e incluso, fuera del.

Por tanto, es una realidad insoslayable que, las nuevas tecnologías han transformado, tanto la gestión y control del personal en la empresa como su fase productiva (Cardona Rubert, 2003) y, es por ello, que es necesario el establecimiento de un equilibrio entre los intereses de ambas partes, puesto que está en juego la vulneración de derechos constitucionalmente reconocidos para los trabajadores.

5 NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Junto al incuestionable crecimiento de los medios tecnológicos en nuestra sociedad, nacen nuevas formas de manejar los datos de carácter personal y, por tanto, nuevos riesgos de uso indebido de esta fuente de información. Es por ello que es necesaria una eficaz protección frente a las nuevas formas de captación y tratamiento de los datos personales (García Murcia & Rodríguez Cardo, 2019).

El primer instrumento vinculante, a nivel internacional, en materia de protección de datos de carácter personal, fue el convenio número 108. Actualmente, a nivel comunitario, hacen referencia al derecho a la protección de datos de carácter personal el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y el artículo 39 del tratado de la Unión (García Murcia & Rodríguez Cardo, 2019).

En el ámbito nacional, la Constitución Española (en adelante CE) no menciona expresamente este derecho, pese a que este unido al artículo 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*"). Por ello, el Tribunal Constitucional se pronunció definiendo el derecho a la protección de datos como un derecho que consiste en "*un poder de disposición y de control sobre los datos personales*[1]"

En un contexto donde las relaciones en el trabajo (procesos de selección, durante la vigencia del contrato, obligaciones fruto de la relación laboral etc.) se basan, en gran parte, en el intercambio y captación de datos de carácter personal, nace el Reglamento (UE) 2016/679, del Parlamento Europeo y el Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).

Continuando con la legislación en protección de datos personales, nos encontramos dos vertientes, la normativa aprobada por la Unión Europea, donde nos encontramos el ya mencionado Reglamento (UE) 2016/679 y, por otra parte, la normativa nacional, donde nos encontramos con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (en adelante LOPDGDD). Añadir, que a

[1] STC, de 30 de noviembre 2000 (Recurso de Inconstitucionalidad 201/19993219/1993, 226/1993, 236/1993) y STC, de 30 de noviembre 2000 (Recurso de Inconstitucionalidad 1463/2000).

pesar de que ambas normativas tienen un carácter general, son tremendamente importantes para la regulación de las relaciones laborales (Ortega Giménez, 2019).

6 LA DOCTRINA EN EL CONTEXTO DE LA VIDEOVIGILANCIA. LA EVOLUCIÓN HASTA LA ACTUALIDAD

No se ha seguido un criterio único a lo largo de los años en cuanto al tecnocontrol, y especialmente, en materia de la videovigilancia. Consecuencia de esta problemática, el derecho a la intimidad, al secreto de las comunicaciones y a la libertad informática, han sido derechos discutidos por cuanto, en determinadas ocasiones, estaban siendo vulnerados en el marco laboral fruto de malas praxis empresariales (Cabeza Pereiro, 2018).

A la vista de la masiva incorporación de las tecnologías de la información y comunicación a la producción de las empresas, y la prácticamente nula regulación en dicha materia en el marco laboral, los tribunales se ven obligados a marcar un camino en el establecimiento del equilibrio entre el poder de control del empresario y los derechos fundamentales de los trabajadores (Rodriguez Escanciano, 2015). La doctrina judicial ha ido evolucionando a lo largo de los años, no manteniéndose lineal en el tiempo. Las primeras argumentaciones de los órganos judiciales se centraban en los perjuicios para el derecho a la intimidad y a la propia imagen.

La aparición del derecho a la protección de datos personales, supuso un giro de guion para la presente materia. Así, destacamos 4 periodos, en los cuales priman principios o ideas diferentes:

- **Periodo del principio de proporcionalidad**

A través de este principio, se intentará solucionar las colisiones surgidas entre el derecho de los trabajadores a la intimidad y la facultad de vigilancia y control del empresario. De esta forma, se considerará lícita y por ende, proporcional, la medida del empresario cuando cumpla con los siguientes tres requisitos necesarios (Rodriguez Escanciano, 2015):

1. Juicio de idoneidad: La medida planteada es susceptible de lograr el objetivo perseguido. Es decir, conocer la conducta real del empleado.

2. Juicio de estricta necesidad: No existe otra medida menos limitadora de derechos con el trabajador y que sea igual o más efectiva en cuanto al fin a conseguir.
3. Juicio de proporcionalidad: Si la balanza entre los beneficios que se pueden generar para el interés general, y perjuicios que pueda suponer para otros bienes o valores en conflicto es favorable, por cuanto supone un mayor beneficio que perjuicio.

El propio principio de proporcionalidad cohabita, en la presente etapa, con la figura de la información previa obligatoria, pero con excepciones, ya que se permitirá el control oculto a través de la videovigilancia cuando el previo aviso pueda suponer un perjuicio para la consecución del objetivo pretendido (Tillería, 2019). Para complementar el presente análisis y, corroborar dicha información, citaremos las siguientes sentencias, las cuales marcan este periodo:

1. Sentencia del Tribunal Constitucional 98/2000, 10 de abril[2]: La empresa Casino de La Toja, S.A, con el propósito de controlar la actividad laboral que llevaban a cabo sus trabajadores en el centro de trabajo, decide colocar una instalación de micrófonos en el área de la ruleta francesa y de la caja, lugar donde ya se encontraba instalado un sistema de videovigilancia, y de esta forma, completar un sistema completo de control de la actividad laboral. Tras estos acontecimientos, el comité de empresa, posteriormente a la negativa de la dirección del casino a la retirada de los micrófonos, decide impugnar la medida empresarial, llegando hasta el Tribunal Constitucional, previo paso por el Tribunal Superior de Justicia de Galicia, en cuya sentencia se consideró que "*el centro de trabajo no constituye por definición un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores*", entendiendo que no había razón para que la dirección de la empresa no tuviera acceso al contenido de dichas conversaciones y limitando, la privacidad del trabajador, a las zonas de descanso. A raíz de lo acontecido, el Tribunal Constitucional se desmarca del fallo del Tribunal Superior de Justicia de la comunidad de Galicia. Se admite la posibilidad de que, en determinadas circunstancias, sea lícita la medida de incorporar estos mecanismos de control audiovisuales, no siendo en este caso suficiente la utilidad o el beneficio empresarial frente a las restricciones del derecho a la intimidad de los trabajadores afectados. En palabras del Tribunal Constitucional, "*no ha quedado*

[2] STC, de 10 de abril 2000 (Rec.4015/1996).

acreditado que la instalación del sistema de captación y grabación de sonidos sea indispensable para la seguridad y buen funcionamiento del casino", lo cual significa, que se ha rebasado la facultad que al empresario concede el artículo 20.3 del Estatuto de los Trabajadores (en adelante ET) y, además, se ha vulnerado el derecho fundamental a la intimidad consagrado en el artículo 18.1 de la CE, no siendo la medida empresarial conforme al principio de proporcionalidad.

Por lo tanto, la unión mediante un contrato de trabajo entre empresario y trabajador, no debe suponer para este último la pérdida del derecho a la intimidad. La medida empresarial, restrictiva de derecho, debe superar el test de la proporcionalidad, pues de lo contrario, como ocurre en el supuesto que nos atañe, la actuación empresarial superaría las facultades que otorga el artículo 20.3 del ET (Tillería, 2019).

2. Sentencia Tribunal Constitucional 186/2000, de 10 de julio[3]: En esta sentencia, el Tribunal Constitucional declara procedente el despido de un trabajador que fue despedido por la empresa Ensidesa tras corroborar, mediante un sistema oculto de videovigilancia, la sospecha de apropiación de dinero de tres cajeros.

En este caso, la propia empresa, tras tener sospechas fundadas, debido al conocimiento de determinados descuadres, por las cuales se estaban cometiendo irregularidades por parte de los trabajadores en las cajas registradoras de una de las secciones de la empresa, contrata a una empresa de seguridad con el fin de llevar a cabo una instalación de cámaras, de forma oculta y sin información previa, para que estas observen exclusivamente a las cajas registradoras de dicha sección, para así corroborar sus sospechas fundadas. El Tribunal Constitucional falla a favor de la corporación Ensidesa, considerando legítima la medida y afirmando que "*la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad*", ajustándose, la medida de seguridad adoptada por la empresa, al principio de proporcionalidad, debido a que, si hubiera habido información previa por parte de la empresa, la medida no hubiera sido eficaz para comprobar que tres trabajadores estaban teniendo un comportamiento irregular.

[3] STC, de 10 de julio de 2000 (Rec.2662/1997).

- **Periodo del principio de información previa**

Entramos en un periodo donde cobra vital importancia el derecho a la protección de datos personales. La problemática del control empresarial a través de la videovigilancia ha alcanzado una nueva dimensión, en la que se valora primordialmente la protección de datos personales[4]. En este contexto, de control empresarial mediante la videovigilancia, adquiere la categoría de fundamental la información o advertencia previa y expresa, puesto que si no se lleva a cabo la información previa al trabajador, se estará vulnerando su derecho a la protección de sus datos personales, tal y como indica el artículo 18.4 de la 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*".

El empresario, al instalar un sistema de videovigilancia en el centro de trabajo, tendrá que tener en cuenta el derecho a la protección de datos de los trabajadores y, evidente es, que tener imágenes de los trabajadores en un dispositivo electrónico supone haber recabado datos personales de los propios trabajadores (Rodriguez Escanciano, 2015), por lo que, a pesar de que el artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos (LO 15/1999 en adelante), respaldara en su momento la no obligación de dar el consentimiento por parte del trabajador en el contexto de una relación laboral, esto no va a suponer que no sea necesaria la información previa acerca de los datos que tiene, que desea recabar, y su finalidad (Rodriguez Escanciano, 2015).

Tomaremos como ejemplo de este periodo la sentencia del Tribunal Constitucional número 29/2013, de 11 de febrero[5]. En esta sentencia se aplica el derecho autodeterminación informativa, debido a que el tribunal no considero legítima la prueba aportada por la Universidad de Sevilla. Esta prueba son imágenes conseguidas a través de cámaras instaladas en los accesos y recintos universitarios, siendo el fin de las cámaras de seguridad, controlar las horas de entrada y salida del trabajo de un trabajador. Gracias a la instalación de las cámaras de seguridad, la Universidad de Sevilla se percata de las ausencias continuadas e injustificada del trabajador a su puesto de trabajo, procediendo a partir de los presentes acontecimientos, a sancionarle de empleo y sueldo.

La Universidad de Sevilla, al instalar las cámaras de video grabación, sin haber informado previa y expresamente a los trabajadores de dicha instalación, ni tampoco haber

[4] STC, de 30 de noviembre 2000 (Recurso de Inconstitucionalidad núm. 1463/2000): Antecedente a esta nueva etapa de información previa.

[5] STC, de 11 de febrero 2013 (Rec.10522/2009).

concretado la finalidad y características del tratamiento de datos que iba a llevarse a cabo, vulnera el derecho de los trabajadores a la protección de sus datos de carácter personal proclamado en el artículo 18.4 de la CE. Por lo tanto, el Tribunal Constitucional, al observar el incumplimiento de información previa al trabajador, declara la nulidad de la sanción impuesta.

Se observa un cambio de tendencia en el parecer del Tribunal Constitucional en cuanto a la valoración de los conflictos fruto del control a través de la videovigilancia, en los que el criterio predominante de valoración de dichos conflictos era el principio de proporcionalidad, y donde a través de esta sentencia, se pone énfasis en la información previa, ya que la videovigilancia conlleva una recogida de datos personales, y por tanto, resulta de aplicación el artículo 5 LO 15/1999 ("*derecho de información en la recogida de datos*") y el artículo 6 LO 15/1999, donde se hace referencia a la no necesidad de que en el ámbito de un contrato de trabajo sea necesario el consentimiento. Pero la realidad, como se ha dicho antes, es que esto no supone que no sea necesario informar (Rodriguez Escanciano, 2015).

- **Periodo de flexibilización informativa**

Se produce un cambio doctrinal, donde se observa que se atenúa la obligación de información previa. Claro ejemplo es la sentencia del Tribunal Constitucional número 39/2016 de 3 de marzo[6]:

La empresa Bershka BSK España S.A, tras detectar una serie de irregularidades en una caja registradora, contrata a una empresa de seguridad con el fin de instalar un sistema de videovigilancia con el propósito de controlar dicha caja. Cabe apuntar, que la empresa no informa expresamente a la trabajadora de dicha instalación, pero si coloca un cartel informativo en el escaparate de la tienda, entendiendo el tribunal que el cartel si se coloca en una zona visible. Gracias a la instalación, la empresa Bershka comprueba, en varios días distintos, que una trabajadora ha sustraído dinero de la caja registradora, en concreto, 186,92 Euros. Por este motivo, la trabajadora es despedida disciplinariamente. Posteriormente, la trabajadora demanda a la empresa entendiendo que el despido debe catalogarse como nulo, alegando la vulneración de los derechos fundamentales consagrados en el artículo 18.1 y 4 de la Constitución Española.

[6] STC, de 3 de marzo 2016 (Rec.7222/2013).

A la vista de lo acontecido, desde el Tribunal Constitucional se entiende que hubo información previa, aunque fuese de forma genérica, dando por válido el presente requisito. Esto es debido a que las cámaras de seguridad solo captaban imágenes de una zona del local concreta, la caja registradora. Además, existían sospechas fundadas debido a que la empresa había detectado determinadas irregularidades y, por tanto, también se entendió como cumplido el requisito del principio de proporcionalidad, al entenderse, por lo menos desde el punto de vista del ministerio fiscal, que la medida adoptada por parte de la empresa Bershka era idónea, necesaria y proporcional. Por tanto, la sospecha razonable cobra vital importancia en pro de la flexibilización informativa, convirtiéndose así en base jurídica a la hora de valorar este tipo de conflictos. En este caso se observa que existía, según el Tribunal Constitucional, una sospecha razonable porque la medida de la empresa iba dirigida a la protección de su patrimonio, y no con vistas a monitorizar el trabajo de la recurrente (Tillería, 2019).

En definitiva, la facultad de control empresarial reconocida en el artículo 20.3 del ET, permite en el ámbito de la videovigilancia, la posibilidad de tratamiento de datos personales de los trabajadores cuando la finalidad sea legítima y no suponga un abuso de derecho y, por tanto, aunque esto no requiera un consentimiento expreso, si nos encontramos con el deber de información reconocido en el artículo 5 LO 15/1999.

- **Sospechas razonables. A propósito del caso López Ribalda (Sentencia TEDH de 17 de octubre de 2019)**

La doctrina naciente a raíz del parecer del Tribunal Europeo de Derechos Humanos (TEDH en adelante) ha traído mucha polémica, puesto podría estar asentando las bases de una vigilancia oculta y clandestina sobre los trabajadores, restringiendo por ende su derecho fundamental al respeto de la vida privada, puesto que dicha sentencia no parece tomar en consideración el artículo 5 ("*derecho de información en la recogida de datos*") de la anterior Ley sobre protección de datos (LO 15/1999).

En el caso a analizar, la dirección de un supermercado detecta irregularidades en los stocks del supermercado y en las cifras de venta, comprobando así unas pérdidas que ascienden, en junio de 2009, a la cantidad de 24614 €. Tras dicha situación, la empresa procede a instalar dos tipos de cámaras de vigilancia, unas visibles y otras ocultas. De la instalación de las cámaras de videovigilancia visibles son informados los trabajadores, justificando dicha medida en las sospechas por robo. La instalación de las cámaras ocultas

no se puso en conocimiento ni de los representantes legales ni de los trabajadores. Posteriormente, al confirmar la empresa sus sospechas de robo, fueron despedidos 14 trabajadores del supermercado, entre ellos, las 5 trabajadoras demandantes del proceso judicial que estamos analizando.

A raíz de lo acontecido, las 5 trabajadoras demandan a la empresa alegando una violación del derecho a la protección de la vida privada, creyendo oportuno que no deberían ser admitidas como prueba las grabaciones realizadas mediante las cámaras ocultas. En este sentido, el juzgado de los social fallo a favor de la empresa declarando procedentes los despidos, al igual que en siguiente instancia el Tribunal Superior de Justicia de Cataluña, puesto que entendió que, a raíz del artículo 5 de la derogada Ley sobre protección de datos, "*el incumplimiento de la obligación de notificación era una mera cuestión de legalidad ordinaria que puede traer como consecuencia una sanción administrativa para el empleador pero nunca la expulsión del material probatorio del procedimiento judicial*" (Zaragoza Tejada, 2020).

Una vez llevado el asunto a la sección tercera del TEDH por vulneración del derecho a la intimidad, el propio tribunal declaro que no compartía el parecer de la justicia española, puesto que, si consideraba que se había vulnerado el artículo 8 del Convenio Europeo de Derechos Humanos, justificando dicho parecer en virtud de:

a) Incumplimiento de la empresa en cuanto al deber de información a los trabajadores sobre la existencia de dispositivos de recogida y tratamiento de datos personales.
b) Las cámaras de vigilancia se dirigían a una generalidad de empleados de la empresa, y no hacia una persona en concreto. También, la medida fue adoptada sin límite de tiempo y durante toda la jornada laboral.

Finalmente, la gran sala del TEDH adoptó una postura similar a la de la justicia española, argumentando que la expectativa de privacidad que las empleadas pudiesen tener era limitada puesto que su actividad profesional ya se desarrollaba de cara al público, consiguiendo dichas pruebas en sus puestos de trabajo y no en lugares privados, como pueden ser, los aseos o vestuarios.

Ante esta situación, el TEDH declara que la vigilancia a través de cámaras fue legítima y justificada, puesto que existían sospechas razonables de robo, que la medida no fue excesiva en cuanto a la duración de la misma, puesto que solo se alargó 10 días y finalizo en cuanto los culpables fueron identificados, que la medida de control utilizada por el

empresario debe ser considerada como necesaria para la identificación de los sospechosos y que las imágenes captadas solo fueron mostradas al representante de la empresa y representante sindical.

Por lo tanto, a la vista de los acontecimientos, es necesario elaborar un juicio y ponderar los elementos concurrentes en cada caso, ya sea el lugar de colocación de las cámaras de vigilancia, duración de la medida, sospechas fundadas de ilícito etc., puesto que desde la gran sala se han decantado por la valoración de estos elementos en su conjunto, dejando claro que, aunque no se cumplió la legalidad vigente al completo, la información suministrada por las cámaras no hubiese sido la misma si se hubiera informado previamente a los trabajadores sobre la colocación de las mismas (Zaragoza Tejada, 2020).

7 ADAPTABILIDAD DE LA NORMATIVA EN PROTECCIÓN DE DATOS AL ÁMBITO LABORAL

La adopción de instrumentos digitales por la empresa, conlleva a la realización de un análisis con una doble vertiente. Una positiva, en cuanto a una mayor facilidad para alcanzar la máxima productividad y eficiencia posible por parte de la empresa, ya sea en la actividad productiva o en la gestión de los empleados[7]. La otra vertiente será negativa, debido a que al juntar el poder de dirección que corresponde al empresario, con las innumerables posibilidades que ofrece la nueva tecnología, el resultado podría derivar peligrosamente en una vulneración de derechos pertenecientes a los trabajadores.

El poder de la informática ofrece al empresario la posibilidad de recabar y tratar información personal de los empleados. La informática hace posible juntar en un soporte electrónico datos personales de los trabajadores, los cuales, sin el poder informático, serían prácticamente imposibles de conseguir, además de poder tratar esta información personal sin el conocimiento ni consentimiento de los propios empleados. Como último apunte en este sentido, hay que añadir, que muchos de esos datos recabados, nada tienen que ver con las obligaciones laborales o capacidades profesionales de los trabajadores (Rodriguez Escanciano, 2015).

[7] Ventajas en cuanto a una gestión informatizada del personal para realizar determinadas gestiones en nombre del trabajador, como puede ser el correspondiente pago de la cuota de la seguridad social; ventajas, también, en relación a administrar la gran cantidad de datos de los trabajadores recabados por la empresa sobre formación, aptitudes físicas y mentales etc.

Ante la ausencia de una normativa específica en cuanto a protección de datos en el marco laboral, la idoneidad, llegaría encontrando un punto de equilibrio entre, el poder empresarial, optimizando la vertiente positiva, y la protección adecuada de los derechos de protección de datos en favor de los trabajadores.

En un contexto de ausencia normativa concreta, debemos guiarnos por la normativa general de tratamiento de datos automatizados, es decir, por el RGPD (Rodriguez Escanciano, 2015).

El artículo 88 del RGPD dispone que los estados miembros, en cuanto al tratamiento datos en el ámbito laboral, tendrán la potestad de, a través de sus disposiciones legislativas o convenios colectivos, "*establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral*". En este sentido, se pueden fijar normas en materia de contratación del personal, gestión de los empleados, seguridad del trabajo etc. Todo esto, través de normas que protejan y preserven, tal y como se indica en su apartado 2, "*la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo*".

Postergando, para más adelante, la forma con la que los convenios colectivos pueden preservar los derechos fundamentales en cuanto a protección de datos personales de los trabajadores se refiere, hay que decir, que a la vista de la evolución tecnológica, y el poder que ésta permite a los empresarios y/o responsables de tratamiento, aparecen, además del derecho a la intimidad consagrado en el artículo 18.1 CE, el derecho a la autodeterminación informativa, consagrado en el artículo 18.4 CE, según el cual, "*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*". Esto se traduce en la capacidad que tenemos, como propietarios de nuestro patrimonio informativo-electrónico, de decidir la persona o entidad que puede acceder a nuestros datos, acumularlos, tratarlos etc. (Rodriguez Escanciano, 2015). Por lo tanto, el derecho a la autodeterminación informativa supondrá que el trabajador debe tener el conocimiento, mediante ficheros automatizados, de que información suya hay sido recabada, como la han conseguido, su finalidad, el destinatario de los datos personales etc.

Dejando de lado el derecho de autodeterminación, según afirma el artículo 5.1 a) RGPD, "*los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado*". Además, dentro del mismo artículo, según su apartado 1 c), deberán ser "*adecuados, pertinentes y limitados a los necesarios en relación con los fines para los que son tratados*". Por tanto, se exige que exista un motivo lícito y justificado para recabar información personal del trabajador, además de ser el motivo concreto y no abstracto o indeterminado. En relación con la finalidad, también se prohíbe, en estos términos, la finalidad indeterminada en el trabajo para evitar posibles engaños a los trabajadores con el fin de recabar datos personales que de nada servirán para mejorar la actividad productiva (Rodriguez Escanciano, 2015).

Los datos personales, en virtud del artículo 5.1, apartados a) y b), deberán de ser tratados lícitamente y recogidos con un fin legítimo, puesto que recabar y tratar datos personales ilegítimamente queda completamente prohibido. Este supuesto se puede dar, por ejemplo, en los procesos de selección de personal, en donde el responsable de recursos humanos o el propio empresario, pueden verse incitados a investigar en la vida personal del candidato, obteniendo y tratando datos con la categoría de sensibles, como pueden ser la ideología política, afiliación o no a un determinado sindicato, datos acerca de la vida sexual del candidato etc. Por lo tanto, tenemos presente el principio de legalidad en la recogida y tratamiento de datos, el cual tiene que ser respetado por el empresario o responsable de tratamiento (Rodriguez Escanciano, 2015).

En cuanto a los datos recabados, estos, en virtud del principio de exactitud, deben ser exactos, y debiendo, en su caso, ser actualizados correctamente, adoptándose las medidas pertinentes para suprimir o rectificar los datos inexactos respecto a los fines para los que se tratan.

En cuanto a los derechos en protección de datos aplicables a los trabajadores en el ámbito laboral, destacamos los siguientes:

- Derecho de acceso (artículo 15 RGPD): El trabajador tiene derecho a conocer, del responsable de tratamiento, si se están tratando datos personales que le conciernan y derecho a acceder a ellos, además de conocer el fin de dicho tratamiento, la categoría de esos datos, su destinatario, tiempo durante el que se van a conservar los datos, posibilidad de rectificación o supresión de datos personales, oponerse al tratamiento etc.

- Derecho de rectificación (artículo 16 RGPD): El empleado tiene el derecho de obtener sin dilación indebida del responsable de tratamiento la rectificación de los datos personales inexactos que le conciernan. Tiene también derecho a que se le completen los datos personales que están incompletos. En este sentido, los convenios colectivos aplicables a cada empresa, podrán establecer normas específicas en relación al tratamiento de datos personales de los empleados.
- Derecho de supresión (artículo 17 RGPD): Con la finalidad de proteger al trabajador frente a un tratamiento ilícito de datos en un marco laboral, le es proporcionado al trabajador el derecho de cancelar o suprimir sus datos, ya sea tras finalizar la relación laboral, anular su consentimiento previo, o tras una simple negativa al tratamiento de sus datos. Con el nuevo reglamento general de protección de datos, aparece el derecho al olvido, el cual proclama el derecho del titular de los datos a "*obtener sin dilación indebida del responsable de tratamiento la supresión de los datos personales que le conciernan*". El responsable de tratamiento estará obligado a suprimir sin dilación indebida los datos personales salvo que concurran circunstancias de interés público (Rodriguez Escanciano, 2015). Por lo tanto, a raíz del derecho al olvido y cancelación, está terminantemente prohibido conservar los datos que hagan posible identificar a un trabajador más tiempo del estrictamente necesario para el cumplimiento de la finalidad prevista.

Dentro de la normativa, tanto nacional como comunitaria, se regula el consentimiento que deberá dar el titular de los datos personales, salvo en diversos supuestos, y este es definido, en el artículo 4.11 RGPD como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*", y cuyas condiciones son desglosadas por el artículo 7 RGPD.

Con carácter general, el responsable de tratamiento deberá informar al trabajador acerca del objeto y de la finalidad del tratamiento. Por lo tanto, aparece el concepto del consentimiento informado (Tacón López, 2005). En este contexto, dejamos atrás el consentimiento tácito, propio de la LO 15/1999, para dar paso a un consentimiento que ha de ser mediante una clara acción afirmativa del interesado, debiendo constar de forma "*específica e inequívoca*" para los casos previstos. Uno de estos casos en los que surgirá la obligatoriedad será en el tratamiento de datos con categoría de sensibles.

En la LO 15/1999, en su artículo 6, se recogía el consentimiento como un principio obligatorio salvo en determinados supuestos, pero en la actualidad, en el RGPD, parece ser que no dispondrá de un gran protagonismo[8].

- Derecho a la desconexión digital: En virtud del artículo 88 LOPDGDD, "*los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar*". Todo esto en aras de mejorar y fomentar el derecho a la conciliación de la vida laboral, familiar y personal, y también en relación al posible estrés que pueda sufrir el trabajador debido a que las fuentes de la empresa no cesen en las indicaciones o instrucciones sobre el trabajador, ni fuera del horario laboral. Este derecho queda sujeto a los acuerdos en negociación colectiva o acuerdos de empresa, elaborando el empresario, previa audiencia con los representantes de los trabajadores, una política interna dirigida a los trabajadores. Añadir, como claro ejemplo del derecho a la desconexión digital, la sentencia del Juzgado de lo social nº 23 de Madrid, de 31 de octubre de 2019, donde se impugna una sanción empresarial hacia un trabajador que se había negado a realizar unos cursos formativos "*on line*" en un periodo de descanso (Fernández Orrico, 2019).

8 EL TECNOCONTROL EMPRESARIAL

En la firma contractual de una relación laboral, empresario y trabajador pactan que este último preste su fuerza de trabajo a cambio de una retribución. Al dar comienzo una relación laboral, el empresario tiene la potestad, en virtud del artículo 20.3 del ET, de "*adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*". En un contexto donde las nuevas tecnologías han entrado completamente en los centros de trabajo, éstas, pueden aportar tanto positiva como negativamente.

La forma positiva viene dada, sin ninguna duda, por la mejoría que han aportado al proceso productivo y organizativo de las empresas. Desde la perspectiva negativa, no hay

[8] STC, de 3 de marzo 2016 (Rec.7222/2013): Observamos que el necesario consentimiento del trabajador queda relegado a un segundo plano.

que obviar el poder que las nuevas tecnologías conceden al empresario en cuanto al intensificado y personalizado control al que se le puede someter al trabajador, poniendo en peligro derechos fundamentales propios del trabajador y de cualquier ser humano, como son la "*libertad, la dignidad, la propia imagen, el secreto de las comunicaciones y el derecho a la intimidad*" (Rodriguez Escanciano, 2015).

Por lo tanto, tecnificar e informatizar la vigilancia al trabajador hace posible una gestión personal e individualizada del empleado, el cual se abstendrá de tener ningún tipo de secreto para el empleador, convirtiéndose en un empleado absolutamente transparente para el empresario. Por lo tanto, consiste en encontrar un equilibrio entre el poder de dirección o disciplinario y los derechos de los trabajadores.

8.1 LA VIDEOVIGILANCIA Y LOS DISPOSITIVOS DE GRABACIÓN DE SONIDO

La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) persigue garantizar la protección del derecho a la intimidad frente al "*uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo*". El artículo 22 LOPDGDD regula el tratamiento de imágenes obtenidas mediante video cámaras para proteger la seguridad de las "*personas, bienes e instalaciones*".

Observando el artículo 64 ("*derechos de información y consulta*") apartado 5.f) del ET, los representantes de los trabajadores "*tendrán derecho a emitir un informe previo a la ejecución por parte del empresario de las decisiones adoptadas por este*" en materia de implantación y revisión de sistemas de control. Este artículo, nos deja entrever , por lo tanto, que los representantes legales de los trabajadores deberán recibir la pertinente comunicación previa a la adopción e implantación de las medidas de control, entre ellas, la videovigilancia (Rodriguez Escanciano, 2015). Aunque también es verdad que en determinadas circunstancias la información previa, ya sea a los trabajadores directamente o a los representantes de estos, puede evitar la eficacia de las correspondientes medidas y herramientas de control, y por consiguiente, no conseguir su finalidad, la cual sería la reafirmación en las sospechas fundadas de conducta irregular.

En las circunstancias del artículo 22 LOPDGDD ("*seguridad de las personas, bienes e instalaciones*"), la obligación de informar sería dada por cumplida situando un dispositivo informativo en una localización visible. Por ejemplo, a través de un cartel.

Mientras en el segundo caso, observando el artículo 89 LOPDGDD, se exige que se informe de manera expresa, por parte del empresario, a los trabajadores y/o sus representantes legales sobre la adopción de la medida de control. Es cierto que la ley no contempla explícitamente que el empleador deba de detallar la finalidad de la medida, pero sí debería entenderse que informar también sobre la finalidad forma parte del núcleo esencial de la obligatoriedad de información previa del empleador (Rodriguez Escanciano, 2015). La complejidad aparece cuando el artículo 89 LOPDGDD, en su apartado primero, afirma que "*en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 ("dispositivo informativo en lugar suficientemente visible") de esta ley orgánica*". Por lo tanto, parece que esta regulación está rectificando la interpretación realizada por el Tribunal Constitucional en la sentencia número 29/2013 y asentando las bases creadas por la STC 39/2016 (Caso Universidad de Sevilla y Bershka España).

Por último, en virtud del artículo 89.2 LOPDGDD, cabe añadir la imposibilidad de la instalación de estos sistemas de control con el fin de vigilar a sus trabajadores en "*lugares destinados al descanso o esparcimiento de los trabajadores*".

8.2 REGISTRO DEL ORDENADOR, PROPIEDAD DE LA EMPRESA, EN EL CENTRO DE TRABAJO

La empresa puede proveer a los trabajadores de ordenadores como herramienta para la actividad profesional. A partir de aquí, son numerosas las empresas que hacen de esto una herramienta de control informático sobre los trabajadores, realizando controles directos a través de la vigilancia de su correo electrónico, redes sociales, navegación a través de internet etc.

Cabe preguntarse, en este sentido, si la empresa puede registrar a su antojo los ordenadores de trabajo, puesto que son propiedad de esta y puestos a disposición del empleado con un fin puramente profesional o, por el contrario, el tratamiento legal que merece este asunto gira, al igual que el de las taquillas y efectos personales, alrededor del artículo 18 del ET (solo es posible realizar registros por motivos de "*protección del patrimonio empresarial y el de los demás trabajadores de la empresa, dentro del centro*

de trabajo y en horas de trabajo"), no pudiendo realizar registros libremente, puesto que siempre hay que respetar al máximo la dignidad e intimidad del trabajador.

No falta polémica al respecto entre la doctrina y la jurisprudencia, puesto que los pronunciamientos sobre este asunto han sido dispares, optando en determinados casos por la legalidad de los controles empresariales[9], puesto que son medios de trabajo, propiedad de la empresa, y puestos a disposición del trabajador. Por otro lado, también encontramos pronunciamientos donde dicho registro se condiciona a la información previa[10] al trabajador sobre dichas medidas, y otros donde se exige la aplicación de las garantías ofrecidas por el artículo 18 del ET[11].

Tras la falta de uniformidad en este tipo de enjuiciamientos, el Tribunal Supremo pareció haber encontrado una respuesta a esta problemática tras la unificación de doctrina[12], donde el punto de partida es que el ordenador es un medio, propiedad de la empresa, con una finalidad de uso productiva y puesta a disposición del empleado, pero que su uso queda a juicio del empleador, pudiendo a través de reglamentos de empresa, prohibir un uso con fines personales. Además de poder realizar controles sobre estos medios (Desdentando Bonete & Desdentado Daroca, 2018).

Las conclusiones extraídas de las tres sentencias mencionadas, son la posibilidad, por parte del empresario, de llevar a cabo una prohibición total de uso con fin personal de los medios tecnológicos puestos a disposición de la empresa, la no necesidad de advertir previamente en relación a llevar a cabo un control sobre el ordenador, siempre y cuando existiera esa prohibición reglamentada. Por tanto, esto supone que no se contempla una expectativa de confidencialidad en estos casos.

Tras el caso Barbulescu[13], mencionado posteriormente, es difícil descifrar la repercusión que tendrá en los tribunales nacionales. Mientras tanto, el Tribunal Supremo ha remarcado su posición respecto a este asunto, por él cual, "*si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas*

[9] SSTSJ de Murcia, Cataluña y Sevilla, de 15 de junio 1999 (Rec.620/1999), de 5 de julio 2000 (Rec.1718/2000) y de 9 de mayo 2003 (Rec.591/2003).

[10] SSTSJ de Cataluña y Comunidad Valenciana, de 11 de marzo 2004 (Rec.9725/2003) y de 19 de julio 2005 (Rec.1343/2005).

[11] STSJ de Castilla-La Mancha, de 17 de mayo de 2006 (Rec.1282/2005).

[12] SSTS de 26 de septiembre 2007 (Rec.966/2006), de 8 de marzo 2011 (Rec.1826/2010) y de 6 de octubre de 2011 (Rec. 4053/2010).

[13] STEDH, de 5 de septiembre 2017, donde prevalece la información previa de control sobre los ordenadores, la necesidad de la existencia de prohibición mediante reglamento de empresa.

condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones[14]" (Bartolomé Martín, 2018).

8.2.1 Correo electrónico

Todos somos conscientes del crecimiento del uso del correo electrónico en el trabajo y en nuestra vida personal, puesto que nos sirve de herramienta de comunicación y transmisión de información inmediata, tanto dentro de la empresa como fuera de ella.

Es cierto, que bien utilizado, es una herramienta efectiva para el empresario y el trabajador, con el fin de aumentar la productividad del empleado, pero por otro lado, la dirección empresarial tiene reservas acerca de la conveniencia de su uso, puesto que un uso indiscriminado y personal por parte de los trabajadores, podría poner en peligro la productividad empresarial, puesto que el tiempo dedicado a esta plataforma, en un sentido lúdico, es tiempo inefectivo de trabajo, por lo que disminuiría el rendimiento del trabajador que los envía como del que los recibe.

Continuando en esta dirección, un uso desmedido del correo electrónico podría poner en peligro la seguridad interna de la empresa fruto del intercambio de información confidencial de la empresa, dañando la imagen o competitividad corporativa, afectando tanto a agentes externos como internos de la empresa (Toscani Giménez & Calvo Morales, 2014).

En este caso, el del control del trabajador mediante el correo electrónico, la doctrina opta por la aplicación del principio de proporcionalidad de cara a la declaración, como procedente, este tipo de control y vigilancia. Parece realmente importante conocer si las comunicaciones producidas son a través de un ordenador de uso común, mediante el correo corporativo o utilizando el servidor de la conexión a internet de la empresa, además de si el canal utilizado por el trabajador es abierto o cerrado[15]. Por lo tanto, será necesaria, además de una política restrictiva (o prohibición mediante cláusula de convenio colectivo) en este sentido, una "*necesidad justificada, objetiva y razonable*" (Bonilla Blasco, 2001).

En virtud del artículo 18.3 CE, procede, también en el ámbito laboral, aplicar y proteger el derecho al secreto de las comunicaciones en la empresa. Por lo que el empresario no puede controlar el contenido de las comunicaciones personales ni profesionales del

[14] STS, de 8 de febrero 2018 (Rec.1121/2015).
[15] SSTC, de 7 de octubre 2013 (Rec.2907/2011) y de 8 de febrero 2018 (Rec.1121/2015).

empleado. Este derecho solo podría ser vulnerado a instancias de una resolución judicial, y en términos del órgano judicial social, en virtud del artículo 90.4 de la Ley 36/2011, de 10 de octubre Reguladora de la Jurisdicción Social (en adelante LRJS), solo "*cuando no existan medios de prueba alternativos*" y "*previa ponderación de los intereses afectados mediante un juicio de proporcionalidad*". (Rodriguez Escanciano, 2015).

Por otro lado, el artículo 18.3 CE, en las relaciones laborales, no protege los elementos más cercanos y visibles de la comunicación, como pueden ser la cantidad de mensajes, identidad de destinatario etc.

No faltan sentencias donde se declaran válidas las pruebas y procedentes los despidos mediante una casi libre captación de información personal a través del correo. Destacar la sentencia del TSJ de Cataluña, de 14 de noviembre del año 2000[16], la del Tribunal Constitucional 170/2013[17], de 7 de octubre 2013 o la 241/2012[18].

8.2.2 Navegación por internet

Al igual que el correo electrónico, la navegación vía internet tiene múltiples ventajas en aras de una mayor productividad y rentabilidad a través de la tramitación de ventas, mejora de la imagen empresarial etc., pero como ocurre con el correo electrónico, es un arma de doble filo para la dirección empresarial, puesto que puede restar rendimiento efectivo de trabajo al empleado, suponiendo esto una rebaja de la productividad.

---

[16] STSJ de Cataluña, de 14 de noviembre 2000 (Rec.4854/2000): La empresa se sumerge en las intimidades del correo electrónico del trabajador y, al encontrar contenido de "*«naturaleza obscena, sexista y humorística»*" y "«*continuó enviando mensajes de temática no laboral e incluso promocionó el negocio de su mujer...*»", es despedido tras una falta grave.

[17] STC, de 7 de octubre 2013 (Rec.2907/2011): Se deniega la vulneración del derecho a la intimidad personal consagrado en artículo 18.1 CE, puesto que el uso del correo electrónico con fines personales, mediante "*medios informáticos propiedad de la empresa*", estaba expresamente prohibido por el convenio colectivo aplicable. En este supuesto, el alto tribunal entiende que "*no podía existir una expectativa fundada y razonable de confidencialidad*", puesto que "*la expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización*".

[18] STC, de 17 diciembre 2012 (Rec.7304/2007): La empresa accedió a unos ficheros automatizados donde quedaron guardadas las conversaciones electrónicas entre dos trabajadoras mediante un programa informático de mensajería, el cual había sido instalado en un ordenador de uso común a todos los trabajadores y que no tenía clave de acceso, incumpliéndose así el mandato expreso de la empresa de no instalar programas en el ordenador. Por lo tanto, al no existir previamente esta tolerancia de la empresa sobre el uso personal del ordenador, "*no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado*", rechazándose por lo tanto la vulneración del derecho al secreto de las comunicaciones, puesto que la conversación no había sido llevada a cabo a través de un canal cerrado.

La interacción con internet mediante la visita a diversas páginas web con una finalidad puramente particular no se encuentra protegida por el artículo 18.3 CE (derecho al secreto de las comunicaciones), por lo que la facultad y capacidad del empresario para la vigilancia y control de la navegación por internet es más amplia en cuanto a la intención del empresario de detectar comportamientos irregulares en el uso de esta herramienta informática, mediante el uso de programas especializados, como los programas de monitorización[19] (Rodriguez Escanciano, 2015).

La navegación por internet no supone una comunicación, pero si puede vulnerar, su estricta vigilancia, el artículo 18.1 CE (derecho a la intimidad personal), tal y como se declara en la sentencia 48/2007 del Tribunal Superior de Justicia de Cantabria[20], puesto que a través de este control puedes acceder a datos sensibles del propio empleado (ideología política, vida sexual, creencias religiosas etc.) Por lo cual, a la vista del daño que se puede causar, entra en juego el principio de proporcionalidad a fin de conocer la idoneidad de la medida, la necesidad de la medida de control, además de conocer de si la propia medida es equilibrada y justificada.

8.2.3 Redes sociales

Las redes sociales en el trabajo permiten colaborar y compartir todo tipo de sabiduría técnica relacionada con el trabajo, de forma inmediata y clara. Las redes sociales han conseguido cambiar las relaciones entre nosotros, incluyendo las laborales, aportando una idea de unidad de grupo (Rodriguez Escanciano, 2015).

No solo los trabajadores se pueden aprovechar profesionalmente de ellas, sino que la dirección de la empresa también, ya sea a través de captar potenciales trabajadores mediante los procesos de reclutamiento y selección, proyectando mediante las redes sociales la imagen que gustes dar de la empresa, tareas de marketing etc.

---

[19] Los programas de monitorización son una herramienta, fruto de la evolución informática, que permiten registrar el contenido de los ordenadores, propiedad de la empresa, pero puesto a disposición del empleado, para que de esta forma el empresario pueda conocer las páginas web que visita el empleado, mensajes que manda a través del correo electrónico etc.

[20] STSJ de Cantabria, de 18 de enero 2007 (Rec. 1149/2006): "*tal acopio de datos, en la medida en que entrañaba un control sistemático de los sitios visitados, así como de su frecuencia, tiempo de conexión y navegación, permiten reconstruir aspectos subjetivos relativos a la intimidad del trabajador, y ello excede sin duda de la finalidad declarada: conocer el uso que se hacía de Internet en horas de trabajo, que era el parámetro que debió modular el nivel y la intensidad de la recogida de datos, y que al ser rebasado deslegitima el comportamiento empresarial*".

Por el contrario, son un instrumento que, en el ámbito laboral, no solo pueden ser culpables de reducciones en la rentabilidad y productividad, sino que puede suponer un perjuicio para la empresa en el sentido de publicaciones con comentarios irresponsables, por parte de trabajadores, los cuales pueden minar la imagen de la empresa. También, faltas de respeto a compañeros o superiores mediante comentarios en las redes sociales o revelando determinada información confidencial.

Por otro lado, hay que tener en cuenta que los empleadores están empezando a demostrar incumplimientos de los trabajadores mediante rastros o evidencias que han ido dejando en las redes sociales[21]. El incumplimiento del trabajador es posible que sea grave y culpable, pero la respuesta de los tribunales no debería ser tan automática como un simple "despido procedente", puesto que las circunstancias difieren en cada caso. Puede ser que el perfil desde el que se interactúe este completamente abierto al público, por lo tanto, no se protegerá al trabajador mediante el artículo 18.1 CE (derecho a la intimidad personal) (Rodriguez Escanciano, 2015), o por el contrario, puede que la información haya sido adquirida por la empresa ilícitamente, puesto que el perfil era privado.

Sirva como ejemplo la sentencia del Tribunal Superior de Justicia de Cataluña, donde se declara procedente el despido (por transgresión de la buena fe contractual) de dos trabajadores que, de forma "*completamente premeditada y jocosa*[22]", proceden a la destrucción completa de todo un palet de varios miles de botellas, grabando dicho acto en video y posteriormente subiéndolo a un blog. Cabe citar también la sentencia del Tribunal Superior de Justicia del País Vasco[23], en la que se declara la procedencia del despido a un trabajador, el cual se encontraba de baja laboral por un problema en la pierna, por acudir a todos los conciertos que su grupo musical tenía planeado, saltar encima del escenario y quedar demostrado que el accidente, por el cual está de baja laboral, no fue debido a un accidente doméstico, si no a un resbalón culpa del resbaladizo escenario fruto de la lluvia. Toda esta información quedo demostrada mediante comentarios en redes sociales y la promoción que se llevó a cabo del grupo mediante la sección de un periódico.

[21] Despidos disciplinarios donde la prueba es conseguida gracias a las redes sociales. Estos despidos pueden tener su causa en la competencia desleal, realización de actividades no compatibles con la incapacidad temporal, transgresión de la buena fe contractual etc.

[22] STSJ de Cataluña, de 9 de julio 2009 (Rec.2376/2009).

[23] STSJ del País Vasco, de 26 de octubre 2010 (Rec.2096/2010).

8.3 CONTROL DEL ACCESO Y LOCALIZACIÓN DEL TRABAJADOR EN EL CENTRO DE TRABAJO

8.3.1 Datos biométricos, tarjetas de identificación por infrarrojos y radio frecuencia

El poder empresarial parece no estar solamente limitado al control de la diligencia debida durante la realización de la actividad profesional, sino que, como veremos después, los juzgados y tribunales si contemplan la licitud de un control sobre el trabajador en relación al acceso y localización del empleado en la empresa, el cual sería legítimo en función de que su motivación sea la seguridad o "*la comprobación del efectivo cumplimiento de las obligaciones*"[24].

Las tarjetas de identificación tienen el objeto de controlar los movimientos que tiene el trabajador (incluidos la entradas y salida del centro de trabajo) y su ubicación en un momento determinado. Esto es posible mediante una tarjeta individual, qué tras acercarla a un lector, el trabajador podrá acceder al centro de trabajo, a una determinada sala etc., conociendo, por lo tanto, las horas exactas en las que el trabajador realizó esos movimientos.

Por cuanto a la radiofrecuencia, a través de un sistema de seguimiento y almacenamiento de datos, sin necesidad de "*contacto físico ni interacción visible entre el lector y la etiqueta*" (Rodriguez Escanciano, 2015), consigue también el objetivo de la localización.

Otro instrumento, cada vez más usado en las grandes empresas, son los sistemas de registro biométricos, que son usados para controlar el cumplimiento de acceso a las instalaciones de la empresa y del horario de trabajo a través de la captación y análisis de aspectos físicos (huellas dactilares, el iris la voz etc.) o de la morfología del rostro del empleado.

Tomando como punto de partida el artículo 4.1 RGPD, son datos personales "*toda información sobre una persona física identificada o identificable (el interesado)*". En este sentido, y teniendo en cuenta que el presente artículo afirma que se puede identificar a una persona mediante "*datos de localización*" o "*elementos propios de la identidad física o fisiológica*" (Rojas Rosco & López Carballo, 2018), cabe preguntarse si se le está dando suficiente importancia a lo que supone para un trabajador estar completamente sometido a un estricto control, por parte de "un gran ojo", de manera exhaustiva y a tiempo real.

[24] STSJ de Cantabria, de 21 de febrero de 2003 (Rec.763/2002).

Cabe decir, qué en la fase de recogida y tratamiento de los datos conseguidos mediante los controles biométricos, se están poniendo en peligro derechos fundamentales de los empleados, como el derecho a la intimidad personal (Rodriguez Escanciano, 2015).

Por otro lado, parece que los tribunales están pronunciándose a favor de la licitud de estas formas de control[25], por la cual se da validez a la implantación de un sistema de control mediante la "*lectura biométrica de la mano por un escáner mediante rayos infrarrojos y en la transformación de su imagen tridimensional en un algoritmo plasmado*"[26].

Por lo cual, parece que no habrá vulneración de la vida privada del trabajador siempre y cuando estemos ante "*medidas adecuadas, pertinentes y no excesivas*" (Rojas Rosco & López Carballo, 2018).

8.4 SISTEMAS DE GEOLOCALIZACIÓN

Esta herramienta de control laboral es sobre todo utilizada cuando el empleado realiza su jornada laboral fuera de su centro de trabajo, como pueden ser los transportistas. La geolocalización permite que la empresa conozca la ubicación del empleado, usando para ellos sistemas de localización en el teléfono móvil, GPS en el vehículo de la empresa usado por el empleado, "*microchips insertados en tarjetas identificativas que lleva consigo el trabajador"* etc. (Rojas Rosco & López Carballo, 2018).

Los sistemas de geolocalización, proporcionan a quien los usa en beneficio propio datos personales, especialmente sensibles, que pueden entrar en colisión con el derecho a la intimidad y con la privacidad del afectado. De hecho, la Agencia de protección de datos en su Informe 193/2008 indica que los datos que hayan sido adquiridos mediante un sistema de geolocalización, son asociados a datos de carácter personal de una persona identificada o identificable, por lo que se deben seguir las reglas y protecciones previstas por el Reglamento General de Protección de Datos (Rodriguez Escanciano, 2015).

Por los diferentes pronunciamientos de los tribunales, los cuales son dispares, si parece clara la necesidad de información previa y expresar la finalidad[27] de la medida de control

[25] STSJ de Murcia, de 25 de enero 2010 (Rec.1071/2009): Validez a esta forma de control en relación al cumplimiento del horario de trabajo.

[26] STS (contencioso-administrativo), de 2 de julio 2007 (Rec.5017/2003).

[27] STSJ Castilla-La Mancha, de 23 de marzo 2015 (Rec.1775/2014): El demandante (trabajador) reclama la vulneración del derecho fundamental a la intimidad personal tras la instalación, en el coche que utiliza para realizar su actividad profesional, de un sistema GPS de cómo medio de vigilancia. El fallo declara

que se va a ejercer sobre él trabajador. En este sentido, cabe citar el artículo 90.2 LOPDGDD, el cual expresa la necesidad de "*informar de forma expresa, clara e inequívoca a los trabajadores*". Si se incumple dicha condición, la medida del empleador podría colisionar con los derechos fundamentales a la intimidad y protección de datos, siendo en este caso, la prueba ilícita[28]. (Ortega Giménez, 2019).

No parece necesario que se produzca un consentimiento expreso del trabajador, salvo que el uso del sistema GPS y, en consecuencia, el tratamiento de estos datos de carácter personal, se produzcan fuera del tiempo de trabajo o jornada laboral, puesto que la justificación de esta medida de control radica en la facultad de supervisión del empleador[29] (Quílez Moreno, 2019).

9 POSIBLE VULNERACIÓN DE LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES FRUTO DE UN EXHAUSTIVO CONTROL EMPRESARIAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

Vivimos en una sociedad dependiente de las TICs[30], las cuales crecen día a día en cuanto a la influencia que tienen en nuestras relaciones y, en general, en nuestras vidas.

Las relaciones laborales no se quedan atrás en cuanto al crecimiento de las TICs y la influencia que ejercen. Por lo tanto, no debemos quedarnos atrás en relación a la necesidad de regular y proteger a los trabajadores de nuevas formas de vigilancia y control impersonal. Nacen, por tanto, los "*derechos on line*" de los trabajadores, reconocidos constitucionalmente mediante el artículo 18.4 CE, el cual dispone que "*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*".

Los artículos 33 y 38 de la CE, los cuales reconocen el derecho de propiedad y la libertad de empresa respectivamente, junto al artículo 20.3 ET, donde se legitiman las "*medidas oportunas de vigilancia y control*", no deben ser utilizadas para llevar a cabo, injustificadamente, un control y vigilancia exhaustiva, colisionando así con derechos fundamentales consagrados en el artículo 18 CE y en especial, el derecho a la intimidad

inexistencia en cuanto a la vulneración del derecho fundamental, puesto que se cumplieron los requisitos legales; "*se informó suficientemente al trabajador de su instalación y de la finalidad que con la misma se persigue*".

[28] STSJ de Madrid, de 21 de marzo 2014 (Rec.1952/2013).

[29] STSJ de Asturias, de 27 de diciembre 2017 (Rec. 2241/2017).

[30] Tecnologías de la Información y la Comunicación.

y al secreto de las comunicaciones. Por otro lado, el derecho a la intimidad también es recogido de forma específica para el ámbito laboral por el artículo 4.2 e) ET (Catoira, 2011).

Por lo cual, no se trata de primar determinados derechos sobre otros, si no de encontrar un equilibrio entre la facultad de control del empresario y los derechos fundamentales de los trabajadores. Afirmación, que queda demostrada observando el artículo 90.1 LRJS, donde afirma que "*podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos*". Por lo tanto, no es posible en todos los casos, ante una conducta irregular del trabajador, alegar una vulneración de la vida íntima de cara a encontrar la impunidad laboral de su conducta[31]. Se entiende, por lo tanto, que el límite se encuentra en los procedimientos que hayan sido utilizados para la obtención de la prueba, los cuales no pueden suponer una vulneración de los derechos fundamentales.

En una relación laboral, tanto para el trabajador, como para el empresario, surgen una serie de derechos y obligaciones recíprocas que condicionan el ejercicio del derecho. Por lo tanto, *"manifestaciones del mismo que en otro contexto pudieran ser legítimas, no tienen por qué serlo necesariamente en el ámbito de dicha relación*[32]" (Catoira, 2011).

Ante esta situación y, según la doctrina del Tribunal Constitucional, para que sea posible limitar derechos fundamentales, hay que seguir el ya mencionado principio de proporcionalidad e información previa. Esto obliga a realizar un "*juicio casuístico*" siempre que un empleado sienta que está siendo objeto de una vulneración de derechos fundamentales (Rodriguez Escanciano, 2015).

"*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Así dice el artículo 18.3 CE acerca de la inviolabilidad de las comunicaciones. En el ámbito laboral no es tan sencillo, puesto que el conflicto de derechos (trabajador-empleador) puede llegar en el momento en el que el trabajador usa los medios de comunicación que la empresa pone a disposición del trabajador, con un fin profesional, como forma de comunicación personal. En este contexto, los derechos de ambas partes, constitucionalmente reconocidos, pueden entrar en colisión en el momento en que el empleador use sus herramientas y facultades de

[31] STSJ de Andalucía, de 22 de junio 2001 (Rec.124/2001).

[32] STC, de 15 de diciembre 1983 (Rec.69/1983).

vigilancia y control para comprobar el uso que da el trabajador a los medios electrónicos que fueron puestos a su disposición (Catoira, 2011).

En este sentido, los tribunales, dan prioridad a la política de la empresa[33], cerciorándose de la prohibición o no del uso personal de los medios electrónicos propiedad de la empresa. Comprobamos, por lo tanto, la importancia que ostenta en este sentido la negociación colectiva y la política empresarial.

En cuanto al derecho de protección de datos, íntimamente ligado con el derecho de intimidad, tiene también que convivir con la facultad de vigilancia y control que el ET, en su artículo 20.3, confiere al empresario. Por lo tanto, para realizar la ponderación correspondiente, los tribunales acostumbran a utilizar el principio de proporcionalidad.

Por otro lado, la LOPDGDD, desde su artículo 87 hasta el 90, ambos incluidos, regula el derecho a la intimidad en relación al uso de dispositivos digitales en el ámbito laboral (cierto es, como indica el artículo 87.2 LOPDGDD, que "*el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos*"), a la desconexión digital (artículo 88), a la intimidad frente al uso de dispositivos de videovigilancia y grabaciones de sonido y geolocalización (artículos 89 y 90 respectivamente). Estos derechos podrán ser mejorados por los convenios colectivos, incluyendo así, garantías suplementarias en relación al tratamiento de datos personales y protección de los derechos digitales de los trabajadores en el ámbito laboral. (Aranzadi Instituciones).

Para finalizar, cabe añadir, tomando como ejemplo la sentencia TEHD de 5 de septiembre de 2017[34] en el caso Barbulescu, que la jurisprudencia europea considera que las comunicaciones efectuadas por el empleado en su respectivo puesto de trabajo, están

---

[33] STSJ de Catilla y León, de 20 de diciembre 2006 (Rec.2005/2006): El tribunal consideró la medida disciplinaria sobre el empleado como "*actuación excesiva de la empresa*" el despido al empleado por utilizar el ordenador de la empresa "*para acceder a internet para asuntos personales*", puesto que "*no constaba una prohibición expresa y absoluta*" por parte de la empresa en cuanto al acceso a internet con fines personales.

[34] TEDH 5 de septiembre 2017 (Demanda núm.61496/2008): Se consideró que la empresa había incurrido en una violación a la vida privada, y en especial, al secreto de comunicación, del trabajador, puesto que no se llegó a comprobar con certeza si el empresario comunicó con anterioridad al demandante la posibilidad de que las comunicaciones mediante Yahoo Messenger fueran controladas en el marco del control del trabajo efectivo, así como de la naturaleza y grado de intrusión en la vida privada y correspondencia del demandante. Por lo tanto, se produjo, a ojos del tribunal, un desequilibrio entre "*los intereses del empleador y el derecho del demandante al respeto de su vida privada*".

dentro de la consideración de lo que es su vida privada, por lo cual, el empleador solo tendrá la potestad de controlar, vía informática, las comunicaciones del trabajador cuando exista, además de una prohibición expresa del uso de internet con una finalidad personal, un aviso previo empresarial en virtud del cual existiese la posibilidad de que la empresa tome las medidas necesarias en este sentido, y por otro lado, la necesidad de que estas medidas sean justificadas, apropiadas y necesarias para lograr el objetivo propuesto, respetando así, la vida privada y el secreto de las comunicaciones del empleado (Aranzadi Instituciones).

9.1 LA INDEMNIZACIÓN POR VULNERACIÓN DE LOS TECNO DERECHOS DE LOS TRABAJADORES

A raíz de lo expuesto con anterioridad, ya es bien sabido que en una relación laboral es necesario garantizar los derechos de los trabajadores y del empresario. No sería justo dejar pasar impunemente un control indiscriminado del empresario sobre el trabajador a través de las nuevas tecnologías, como tampoco lo sería una prohibición sistemática del uso de este tipo de instrumentos de vigilancia y control en favor del trabajador. Por lo tanto, como ya se ha repetido anteriormente, es necesario un equilibrio entre los derechos de las partes de un contrato de trabajo.

En este sentido, el ordenamiento jurídico ha creado una forma de actuación ante la vulneración de los derechos fundamentales de los trabajadores mediante el control y vigilancia del empleador a través de la tecnología. Aquí, es donde entra el juego la Ley 36/2011, reguladora de la jurisdicción social.

Hay que comenzar mencionando la regla de la carga de la prueba, puesto que, según la misma, el empleado deberá aportar un indicio razonable que demuestre que la acción empresarial vulnera su derecho fundamental. A partir de este momento, el demandado deberá demostrar que su acción esta legítimamente fundamentada en causas ajenas a la lesión de derechos fundamentales. Es decir, la carga de la prueba recae en mayor medida sobre el empresario (Rodriguez Escanciano, 2015).

La Ley Reguladora de la Jurisdicción Social, siempre que el litigio se encuentre dentro del marco del orden social, será la encargada de conocer, junto con la jurisdicción social, los litigios acerca de la tutela de los derechos fundamentales.

El artículo 179.3 LRJS menciona que además de los determinados requisitos generales propios de la LRJS, la demanda "*deberá expresar con claridad los hechos constitutivos de vulneración, el derecho o libertades infringidos y la cuantía de la indemnización pretendida, en su caso, con la adecuada especificación de los diversos daños y perjuicios, a los efectos de lo dispuesto en los artículos 182 y 183, y que, salvo en el caso de los daños morales unidos a la vulneración del derecho fundamental cuando resulte difícil su estimación detallada, deberá establecer las circunstancias relevantes para la determinación de la indemnización solicitada, incluyendo la gravedad, duración y consecuencia del daño, o las bases del cálculo de los perjuicios estimados para el trabajo*". En este aspecto, cuando probar la cuantía del daño resulte difícil o costoso, corresponderá al juez determinar la cuantía indemnizatoria de manera prudencial, y de esta forma, compensar al demandante y restablecer a éste, en la medida en que se pueda, en la "*integridad de su situación anterior*", tal y como indica el artículo 183 LRJS. Es el artículo 183.1 LRJS, el que reconoce que ante la existencia de una sentencia que declare la vulneración del derecho fundamental, será el juez quien "*deberá pronunciarse sobre la cuantía de la indemnización*".

Para finalizar, y según indicó la sentencia del Tribunal Supremo de 12 de diciembre de 2011, cabe afirmar que la indemnización deberá ser "*suficiente, idónea y proporcionada a la lesión*", con el objetivo de compensar y reparar a la víctima. De otro lado, intentar prevenir daños futuros. Por lo cual, quedan excluidas las indemnizaciones simbólicas, pudiendo ser perfectamente compatible dicha indemnización, y según indica el artículo 183.3 LRJS, *"con la que pudiera corresponder al trabajador por la modificación o extinción del contrato de trabajo o en otros supuestos establecidos en el Estatuto de los Trabajadores y demás normas laborales*".

10 EL PAPEL DEL CONVENIO COLECTIVO ANTE EL DERECHO A LA PROTECCIÓN DE DATOS

La normativa legal sobre protección de datos debe ser aplicada en el ámbito laboral y tomar en consideración a los trabajadores. Por lo tanto, como veremos, el convenio colectivo es fundamental a la hora de aportar determinadas garantías adicionales y soluciones a favor de los derechos e intereses de los trabajadores.

La importancia del convenio colectivo en cuanto al tratamiento de datos personales de los trabajadores viene marcada por la potestad que le es otorgado por el RGPD, puesto que su artículo 88.1, se remite al convenio colectivo la posibilidad de "*establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral* (…)". También señala el propio artículo, en este caso en su apartado 2, que "*estas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales* (…)".

Por otro lado, desde el artículo 9.2 b) RGPD, se remite a la negociación colectiva a excepcionar la prohibición de tratamiento de datos sensibles en los supuestos en los que el tratamiento de dichos datos sea "*necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral* (…)".

En este sentido, si es usual la incorporación de cláusulas específicas, por parte de los convenios colectivos, donde se detallen ampliaciones en cuanto a derechos de los trabajadores, y en especial, el derecho de información (García-Perrote Escartín & Mercader Uguina, 2018).

Es evidente que la protección sobre los derechos fundamentales de los trabajadores en estos tiempos, donde el empresario dispone de instrumentos tecnológicos que le permiten realizar un control más exhaustivo e impersonal sobre el trabajador, debe ser reforzada, puesto que el derecho a la intimidad, de lo contrario, corre gran riesgo de ser vulnerado. Por supuesto que el trabajador no puede disponer libremente de los medios, propiedad de la empresa, para satisfacer sus propios intereses personales, puesto que de lo contrario se produciría una transgresión de la buena fe, además de poder ser causa de un despido disciplinario. La problemática radica en que el control ejercido por parte del empresario sobre los terminales informáticos puestos a disposición del trabajador podría suponer la lesión de los derechos de intimidad y secreto de las comunicaciones (Quílez Moreno, 2019).

A raíz de lo expuesto y observando la remisión de la norma comunitaria al convenio colectivo, es evidente que la empresa puede regular el uso de los medios informáticos por la vía del convenio colectivo (también mediante instrucciones, códigos de conducta etc.)

Un claro ejemplo de la importancia del convenio colectivo en cuanto al control y vigilancia sobre el trabajador lo encontramos en la sentencia del Tribunal Constitucional

170/2013, de 7 de octubre de 2013, donde se reafirma la idea de que cuando estuviera tipificado como sanción el uso de los instrumentos informáticos para propósitos diferentes a los admitidos, la cláusula que lo indica es vinculante para el empleado y conlleva la prohibición del ya mencionado uso personal[35].

Por lo tanto, tomando como ejemplo esta sentencia, la regulación en el convenio colectivo sobre derechos y prohibiciones de los trabajadores, en este sentido, supone la posibilidad de que la facultad que posee el empresario de vigilancia y control se produzca de forma continuada y con riesgo de colisionar con la "*expectativa razonable de confidencialidad de los empleados en relación con la información presente en los dispositivos informáticos*" (Quílez Moreno, 2019).

11 EL PROCESO DE SELECCIÓN. LOS DATOS NECESARIOS PARA EVALUAR LAS APTITUDES REQUERIDAS

Durante un proceso de selección, nos situamos en la etapa precontractual. Etapa en la cual, por el momento, no hay una relación laboral vigente, pero, sin embargo, el empleador si posee datos personales del candidato al puesto de trabajo.

En este sentido, el tratamiento de los datos de carácter personal del candidato por parte de la empresa será legal, sin que sea necesario el consentimiento previo del candidato, siempre y cuando el interesado haya puesto a disposición de la empresa su currículum. Otro requisito fundamental versará sobre la obligatoriedad de que la finalidad de este tratamiento sea la posible colocación laboral en la empresa y el propio proceso de selección al que se está sometiendo el interesado al puesto de trabajo (Ortega Giménez, 2019).

Dentro de todo proceso de selección en el cual la empresa que busca un potencial empleado y la que realiza el proceso de selección sean la misma, encontraremos dos etapas, siendo la primera la llegada del currículum a la empresa interesada, pudiendo ser recibido por esta mediante una red social de trabajo o directamente a través del interesado. La segunda etapa está compuesta por el propio proceso de selección. Por lo tanto, cuando la empresa recibe por alguna de estas dos vías el currículum de un candidato, podrá

[35] STC, de 7 de octubre 2013 (Rec.2907/2011).

entenderse como válido el consentimiento en relación con el tratamiento de datos personales con la finalidad anteriormente mencionada.

Por otro lado, está completamente prohibido que durante dicho proceso la empresa requiera del interesado datos personales con la categoría de sensible (artículo 9 RGPD), como pueden ser la edad, estado civil, ideología política o la afiliación sindical, puesto que la revelación de este tipo de información podrá ocasionar discriminaciones por motivos no profesionales. Hay que añadir que, durante esta etapa de nuestra existencia, no resultará extremadamente complicado a la empresa conseguir dichos datos, puesto que las personas, por lo general, se exponen en exceso al exterior mediante las redes sociales (práctica más que habitual por parte de la empresa) (Ortega Giménez, 2019).

El objetivo de la segunda etapa será, mediante entrevistas, dinámicas de grupo etc., recopilar la información necesaria acerca de las aptitudes y capacidades de los candidatos. Esto supone la necesidad, por parte de la empresa, de enfrentarse a datos de carácter personal, por lo que su obligación será la de realizar un tratamiento legítimo y cuya finalidad sea únicamente el proceso de selección.

En estas circunstancias, además de avisar al candidato sobre la finalidad del tratamiento (proceso de selección), también cabe mencionar e identificar al responsable del tratamiento y recibir la información pertinente acerca de los derechos que posee, como, por ejemplo, el derecho a la supresión de sus datos personales a la conclusión del proceso. Cabe añadir que la empresa, en determinados momentos, estará interesada en conservar los datos del candidato, ya sea con el fin de incluirlos a una bolsa de trabajo o de remitirlos a otra empresa del grupo. En estos casos la empresa si estará obligada a solicitar el consentimiento expreso al interesado, puesto que el consentimiento tácito concluye en el momento que también lo hace del proceso de selección (Ortega Giménez, 2019).

Cuando hablamos del proceso de selección, cabe mencionar un fenómeno, completamente ilegal, cuya existencia siempre ha sido objeto de debate entre los empresarios y los trabajadores. Hablamos de las listas negras.

Tal y como indica el informe jurídico 2010/0201 de la Agencia Española de Protección de Datos, una lista negra es la "*recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden*

consistir en discriminar a un grupo de personas al excluirlas de la posibilidad de acceso a un determinado servicio o dañar su reputación" (Informe jurídico 0201/2010, 2010).

Vivimos en una época en que las empresas gestionan, desde el inicio de la relación contractual hasta su finalización, todos los datos pertenecientes a sus empleados de una forma informatizada, añadiendo toda esta información en soportes informáticos, con el fin de optimizar sus recursos y así ser más eficientes y competitivos (Poquet Catalá, 2016).

En este contexto, un soporte informatizado en el cual se incluye prácticamente toda la información personal de un trabajador, puede ser fuente de lesión de derechos de los trabajadores, puesto que a través de estas herramientas de gestión puede elaborarse información y son una fuente de potencial tratamiento.

Retomando el asunto de las listas negras, la información y datos personales correspondientes a los trabajadores señalados, son incluidos en un fichero, siendo este propagado por determinadas empresas con la finalidad de imposibilitar el acceso a determinados puestos de trabajo, perjudicando gravemente la salud profesional de los incluidos en ella. Además, puede suponer la vulneración del derecho fundamental al honor y a la protección de datos de carácter personal[36] y perjudicar su reputación.

La ilegalidad de estas malas praxis se fundamentan, por tanto, en la cesión de datos de carácter personal del trabajador a ficheros automatizados sin el conocimiento ni consentimiento expreso del interesado (artículo 5 RGPD), en la discriminación a la persona por circunstancias laborales pasadas y ajenas a la empresa que realiza el proceso de selección al interesado (artículo 14 CE) y en la restricción de la libertad a la elección de profesión y derecho al trabajo (artículo 35.1 CE) (Poquet Catalá, 2016).

12 LOS DATOS ESPECIALMENTE SENSIBLES

El artículo 9 RGPD define los datos personales con categoría especial como aquellos que "*revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos*

[36] STS, de 12 de noviembre de 2015 (Rec.899/2014): El TS declara la vulneración del derecho fundamental al honor y a la protección de datos de carácter personal tras la cesión no consentida por una empresa a otra de datos sobre el despido de un trabajador. Esto causó graves problemas al individuo, puesto que fue rechazado en determinadas entrevistas de trabajo de empresas del sector a causa de la inclusión de la primera empresa en las listas negras, al considerarlo un trabajador conflictivo.

dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física". Además, queda prohibido el tratamiento de este tipo de datos salvo que el interesado diera su consentimiento explícito para ello o se den alguna de las circunstancias definidas en el apartado 2 del presente artículo. A continuación, analizaremos la ilicitud, y sus excepciones, de determinados datos especialmente sensibles.

12.1 RECONOCIMIENTOS MÉDICOS COMO FORMA DE VIGILANCIA

El artículo 22 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales (en adelante LPRL) afirma 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*". Por lo tanto, los reconocimientos médicos formarán parte del presente artículo. Queda constancia, en este sentido, del derecho del empleado a recibir un control de su salud de forma periódica. Esto no quiere decir que el empresario pueda hacer del derecho a la vigilancia de la salud una herramienta de vigilancia y control de las capacidades o aptitudes del empleado[37].

En el momento en el que un trabajador se expone a un reconocimiento médico a cargo de la empresa, corre el riesgo de sufrir una vulneración del derecho a la intimidad personal (artículo 18 CE), por ello, el artículo 22 LPRL dispone, qué en estos casos, siempre habrá que respetar el derecho a la intimidad, a la dignidad y a la confidencialidad de la información sobre el estado de salud del empleado.

Cabe señalar en cuanto a la voluntariedad de los reconocimientos médicos, que como indica el artículo 22.1 LPRL, la vigilancia del estado de la salud "*solo podrá llevarse a cabo cuando el trabajador preste su consentimiento*". Por lo tanto, la regla general será la de la voluntariedad de los mismos.

[37] STC, de 15 de noviembre 2004 (Rec.1322/2000): La empresa procede al despido de una trabajadora "*por falta de aptitud deducida tras un reconocimiento médico de empresa donde se detecta a través de análisis de orina el consumo de drogas*". La Sala Primera del Tribunal Constitucional reconoce la vulneración del derecho fundamental a la intimidad personal al no haber sido informada, no haber dado su consentimiento y no estar justificada la intromisión en la vida privada de la trabajadora. El reconocimiento médico no es una herramienta del empresario de control de la salud de los trabajadores.

Ahondando en la doctrina expuesta sobre el Tribunal Constitucional en esta cuestión, cabe citar de nuevo su sentencia 196/2004, en donde la doctrina se ve realmente reflejada. Cabe decir, por lo tanto, que ante la realización de un reconocimiento médico por parte de la empresa al trabajador, es necesario un consentimiento previo y exteriorizado, no siendo necesaria la forma escrita, puesto que es perfectamente viable el consentimiento verbal y a través de los actos que den a entender inequívocamente dicho consentimiento. Por último, el consentimiento debe ser informado, puesto que la empresa tiene la obligación de informar acerca del alcance, contenido y trato que se va a dar a los resultados obtenidos (Navarro Nieto, 2012).

Por último, es también obligatorio por parte de la empresa, en caso de que pueda afectar de manera más profunda al derecho fundamental de intimidad (debido a que se puedan obtener datos especialmente sensibles, como el consumo de estupefacientes), realizar un acto expreso de información (Navarro Nieto, 2012).

Aunque en la generalidad de los supuestos prime la voluntariedad del trabajador, el derecho a la intimidad no es un derecho absoluto y puede verse limitado en favor de otros derechos constitucionalmente relevantes[38]. Por lo cual, y en este sentido, cabe citar determinados supuestos, dados por el artículo 22.1 LPRL, en los cuales puede resultar obligatorio:

- "*Supuestos en los que la realización de los reconocimientos médicos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores*".
- "*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*".
- "*Cuando así este establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad*".

Como podemos observar, el catálogo de circunstancias por las que deriva el deber del trabajador de someterse al control de la salud es muy amplio, por ello, hay que añadir las matizaciones que se han producido desde el Tribunal Constitucional, donde a través de su sentencia 196/2004, se dan una serie de directrices de cara a resolver las dudas en relación a las condiciones para que dichos reconocimientos devengan en obligatorios:

[38] STC, de 23 de marzo 2009 (Rec.2826/2004).

- "*Indispensabilidad de las pruebas y de su proporcionalidad al riesgo*", puesto que no hay una solución más favorable en aras de preservar derechos de los trabajadores y existe una necesidad objetiva al respecto.
- "*Presencia de un interés preponderante del grupo social o de la colectividad laboral*"

En cuanto a la confidencialidad de los datos médicos, cabe añadir, tal y como indica el artículo 22.4 párrafo 2º y 3º LPRL, "*el acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias*", pudiéndose solo transmitir al empresario con el consentimiento expreso del trabajador.

Por último, solo serán informados el empresario y los responsables en materia de prevención de riesgos "*de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención*".

12.2 LIBERTAD SINDICAL

El artículo 28.1 CE declara la libertad sindical, tanto la individual ("*derecho a fundar sindicatos y a afiliarse al de su elección*") como la colectiva ("*derecho de los sindicatos a formar confederaciones y a fundar organizaciones sindicales internacionales o a afiliarse a las mismas*"). Por otra parte, el artículo 9 RGPD contempla la afiliación sindical del trabajador como un dato especialmente sensible y, por lo cual, queda completamente prohibido el tratamiento de este tipo de datos personales. Esto significa que solo será posible tratar este tipo de datos cuando sea el propio interesado quien dé el consentimiento explícito para el tratamiento de dichos datos personales. En este sentido, hay que exceptuar los ficheros de los que dispone el sindicato, los cuales si contienen los datos relativos a la afiliación de un trabajador. Cabe añadir que el sindicato si debería, en su caso, contar con el consentimiento del interesado antes de ceder dichos datos personales (Rodriguez Escanciano, 2015).

Evidentemente, el empleador siempre es la parte más fuerte de un contrato de trabajo, y mediante el uso de las nuevas tecnologías[39], tiene al alcance la posibilidad de invadir o, por lo menos, poner en peligro el derecho constitucional a la libertad sindical y, de esta forma, obtener el beneficio de la información.

En este sentido, ya sea en un proceso de selección o durante la relación laboral, el trabajador tiene derecho a no proporcionar al empresario la información relativa a su afiliación o no sindical, ideología política o religión, salvo en las empresas de tendencia, puesto que no hay una correlación objetiva entre la afiliación sindical o ideología política con las aptitudes o capacidades profesionales del trabajador. Por tanto, el empresario tendrá prohibido investigar acerca de este tipo de información e incluirla en ficheros automatizados (Rodriguez Escanciano, 2015).

Continuando con el asunto de los ficheros automatizados, cabe mencionar que si podrá ser tratada este tipo de datos especialmente sensibles cuando estas creencias resulten vitales para el diligente desarrollo de la actividad profesional. También resultara legal en los casos en los que la ley nos ofrece la utilidad del tratamiento y gestión de estos datos por parte del empresario (Rodriguez Escanciano, 2015). Este es el caso del supuesto contemplado en el artículo 11.2 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical (LOLS), el cual reconoce que "*el empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad siempre, de éste*". Por tanto, en este supuesto, el empresario, previa solicitud del sindicato, quedará obligado a cooperar al respecto.

Para finalizar, añadir que en el supuesto donde el empleado niega al empresario el acceso a dichos datos personales, podrá ser extraída, en consecuencia, la negativa implícita a que el empleador utilice otros medios para recabar, tratar y ceder dichos datos personales.

12.3 A PROPÓSITO DEL COVID-19

Ante la pandemia global en la que estamos inmersos y, en consecuencia, también una crisis sociosanitaria, es oportuno repasar cual sería la línea diligente de actuación de los

[39] STC, de 17 de febrero 1998 (Rec.3694/1994): Una empresa, con ocasión de una huelga, utiliza sus medios de vigilancia y control a través de cámaras de seguridad, restringiendo y lesionando, de este modo, la libertad sindical de los trabajadores.

trabajadores y empleadores en relación al tratamiento de datos especialmente sensibles, como lo son los relativos a las enfermedades, y más concretamente los relativos al Covid-19.

Se plantea un interrogante en relación con la posibilidad de retomar, por parte de los trabajadores, la actividad económica y profesional sin que ello suponga un riesgo para los mismos. Frente a un contexto donde no es posible, por parte de la empresa, implementar la modalidad laboral del teletrabajo, hay que plantearse si el empresario dispone o no de la facultad de tomar medidas de control de la salud, como, por ejemplo: Control de la temperatura, comunicar al resto de empleados que un compañero suyo sufre dicha enfermedad, realizar preguntas a los trabajadores acerca de si han estado en contacto con personas portadoras o con síntomas comunes del virus, etc. Por tanto, es necesario encontrar un equilibrio entre la necesidad de volver a retomar la actividad laboral, no poner en riesgo la salud de los empleados y, por otro lado, cumplir con la normativa vigente en protección de datos (Muñiz Aguirreurreta, 2020).

Un tema que ha generado cierta controversia, es la toma o no de temperatura a los empleados a la entrada de su centro de trabajo. A estos efectos, cabe mencionar el Considerando (46) del RGPD, el cual habilita el tratamiento de datos de carácter personal afirmando que deberá considerarse lícito cuando pueda responder motivos de interés público o vitales del interesado, incluyendo, dentro de los fines, "*el control de epidemias y su propagación*".

Por otro lado, la base jurídica de la obligación de control de la salud recae también sobre el artículo 21 de la LPRL, afirmando en su apartado 1. a) que: El empresario tiene la obligación de, ante un riesgo grave e inminente para los trabajadores, "*informar lo antes posible a todos los trabajadores afectados acerca de la existencia de dicho riesgo y de las medidas adoptadas o que, en su caso, deban adoptarse en materia de protección*".

Destacar también que, según el artículo 29.1 de la LPRL, "*corresponde a cada trabajador velar, según sus posibilidades y mediante el cumplimiento de las medidas de prevención que en cada caso sean adoptadas, por su propia seguridad y salud en el trabajo y por la de aquellas otras personas a las que pueda afectar su actividad profesional, a causa de sus actos y omisiones en el trabajo*". Añadir, citando el mismo artículo que, no cumplir las correspondientes directrices, en materia de prevención de riesgos, supondrá un incumplimiento laboral. Dicho esto, observamos que, en estas circunstancias, el empleado tiene el deber de no asistir al trabajo si tiene fiebre. Es por ello por lo que el control de la

temperatura parece tener base jurídica en el artículo 20.3 del ET, puesto que el empresario podrá adoptar las medidas oportunas de vigilancia y control en aras de que los trabajadores cumplan sus obligaciones (Ribas, 2020).

Por tanto, en vista a lo anteriormente mencionado, estas medidas de control de la salud (respetando el principio de proporcionalidad) son válidas, puesto que son necesarias para combatir el contagio masivo y proteger la salud del personal de la empresa.

En este contexto de emergencia sanitaria, el empresario sí tendría derecho a saber si el trabajador está o no infectado, siempre y cuando el objetivo de recibir esta información sea cumplir con su obligación (con base jurídica en el artículo 21 de la LPRL) de informar a los trabajadores de los riesgos existentes e implementar, mediante su servicio de prevención, los planes de contingencia necesarios, puesto que el artículo 31 de la LPRL prevé la evaluación de los riesgos laborales, la planificación en materia preventiva, y la aplicación de planes de vigilancia de la salud de los trabajadores frente a los riesgos en el trabajo. Por tanto, el empresario sí que podrá tratar estos datos siempre que siga a rajatabla la normativa comunitaria y nacional, para de este modo, proteger en términos de salud al resto de trabajadores y disminuir el riesgo de propagación del virus (FAQ sobre el COVID-19, 2020).

Por cuanto el empresario dispone del derecho de manejar estos datos, hay que puntualizar que, es fundamental que siempre respete los principios de finalidad y proporcionalidad. En otras palabras, ante la transmisión de este tipo de información, lo ideal sería no identificar al infectado, respetando siempre su privacidad. Por el contrario, claro está que no siempre será posible, por lo cual, en última instancia, si cabría la posibilidad de identificar al afectado (FAQ sobre el COVID-19, 2020).

Por otro lado, las personas trabajadoras que han mantenido contacto con un afectado por el Covid-19 y, por tanto, deben de seguir el protocolo de aislamiento preventivo, si deberán poner a disposición del empresario y del servicio de prevención o delegados de prevención dicha información (FAQ sobre el COVID-19, 2020), puesto que según los artículos 14 y 18 de la LPRL, los trabajadores cuentan con el derecho de información en cuanto a que deberán conocer los riesgos existentes para su salud. Por tanto, el trabajador que haya estado en contacto con un afectado, tenga síntomas comunes de la enfermedad o haya dado positivo en la correspondiente prueba (entre otras situaciones), deberá poner dicha información a disposición del empleador para que tome las medidas oportunas en beneficio del colectivo de la empresa (Ribas, 2020).

Observamos, por tanto, una limitación en nuestro derecho individual ante el conocimiento y tratamiento de estos datos especialmente sensibles, puesto que, poniendo un ejemplo, ante una baja por enfermedad, el trabajador no tiene el deber de informar al empresario sobre las particularidades de su enfermedad.

Esta restricción en el derecho individual del trabajador podría quedar justificada en virtud del artículo 6.1 apartado d): *"el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física*" o e): "*el tratamiento es necesario para el cumplimento de una misión realizada en intereses público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*" RGPD y en virtud de la normativa nacional sobre prevención de riesgos laborales. No olvidando que, a pesar de estar atravesando una situación extraordinaria, la normativa sobre protección de datos sigue vigente y continua siendo de obligado cumplimiento, haciendo referencia, especialmente, al artículo 5 del RGPD, según el cual, los datos deberán ser tratados de forma "*lícita, leal y transparente*", deberán tener una finalidad legítima y ser adecuados y limitados a la finalidad prevista (Muñiz Aguirreurreta, 2020).

Por tanto, si existe una razón objetiva para que el empresario conozca y trate estos datos especialmente sensibles y actúe en función de ellos, protegiendo la salud del personal de la empresa.

13 CONCLUSIONES

La relativamente nueva normativa sobre protección de datos (Reglamento (UE) 2016/679 y Ley Orgánica 3/2018) aparece en nuestra sociedad y, más concretamente, en el mundo de las organizaciones empresariales, en un momento de continuo desarrollo en relación a los sistemas tecnológicos de vigilancia y control utilizados por los empleadores como forma de comprobar el grado de cumplimiento de los trabajadores en cuanto a sus deberes y obligaciones laborales.

A pesar de la cierta tardanza con la que ha llegado dicha normativa, puesto que se venía reclamando una legislación acorde a la evolución tecnológica, sí que tiene, y merecen ser destacados, varios puntos positivos y de interés:

- Una regulación del uso de sistemas de videovigilancia y de grabación de sonidos en el lugar de trabajo, a pesar de que considere que se establecen unos criterios no lo suficientemente claros y objetivos.
- Remisión de la norma a la negociación colectiva. De este modo, a través de diferentes acuerdos, fruto del dialogo social, o cláusulas del convenio colectivo aplicable, surge la posibilidad de ofrecer una ampliación y mayor protección los derechos digitales de los trabajadores, así como delimitar el poder de vigilancia y control tecnológico del empresario sobre los empleados, además de la posibilidad de reducir la incertidumbre en relación a los criterios ponderables de cara a conocer sobre la licitud o ilicitud de la medida empresarial y las pautas marcadas, en este sentido, por la norma.
- Aparición del derecho a la desconexión digital. Con el propósito de garantizar los derechos de conciliación de la actividad laboral y la vida personal y familiar, proteger al trabajador de la fatiga informática, y respetar su tiempo no laborable.
- Deber de advertencia previa en cuanto al uso de cámaras de videovigilancia y de dispositivos de geolocalización.

Cabe señalar, por el contrario, aspectos negativos que me suscita la normativa sobre protección de datos:

- La Ley Orgánica 3/2018 marca un criterio muy difuso en relación a la forma diligente de actuación de los empleadores para restringir y controlar el uso, con fines personales, de los dispositivos digitales puestos a disposición del empleado para llevar a cabo sus obligaciones laborales. Esta es mi opinión debido a que la normativa marca que el empleador deberá regular el uso de dichos dispositivos

teniendo en cuenta, entre otras cosas, los usos sociales. Por otro lado, la norma no señala si el empleador deberá informar previamente antes de llevar a cabo un control sobre dichos dispositivos o, si los medios utilizados para llevar a cabo dicho control deberán ser los menos intrusivos con el trabajador.

- El principio de proporcionalidad, es una buena solución, pero la norma no detalla los criterios que deberán tenerse en cuenta para conocer si la medida de control, utilizada por el empleador, ha superado el juicio casuístico.
- En mi opinión, cumplir con la exigencia de la información previa sobre el empleado, no quiere decir que automáticamente se deba considerar como lícito un control sobre el trabajador, puesto que no se debería renunciar a una expectativa razonable de privacidad por el simple hecho de que el empleador realice la advertencia de control necesaria. Es más, considero que se debería añadir la obligación de utilizar, para dicho control, los medios menos intrusivos posibles.

De esta forma considero que aun contando con una normativa sobre protección de datos, es necesario un mayor desarrollo normativo en cuanto al ámbito laboral se refiere, puesto que dejan demasiadas cuestiones en el aire, pendientes de ser interpretadas, y seguramente, de forma heterogénea, tal y como se ha quedado demostrado tras los últimos pronunciamientos por parte del Tribunal Constitucional o Tribunal Supremo. Por tanto, considero que la legislación debería ser más clara, para que de esta forma, los tribunales no tengan que desarrollar, como vienen haciendo hasta ahora, funciones legislativas.

Por otro lado, tengo la sensación de que los convenios colectivos tienen una importancia vital en este sentido, puesto que, si éstos se provisionaran (en mayor medida) con cláusulas que, de forma expresa, se pronunciaran respecto al grado de prohibición de uso de los dispositivos empresariales con fines personales, a la necesidad de advertencia previa frente a un control a través de sistemas tecnológicos o a la finalidad y alcance de la medida, creo que se evitarían muchos conflictos y se rebajaría el grado de incertidumbre.

Como reflexión final, considero que estamos caminando al filo del precipicio, corriendo un gran riesgo en relación a la perdida de tantos derechos laborales conseguidos a lo largo de muchos años. En mi opinión, un trabajador no puede perder, en el momento que entra a su centro de trabajo, una expectativa razonable de

confidencialidad y privacidad por culpa de una simple política empresarial o advertencia previa.

14 BIBLIOGRAFÍA

Bartolomé Martín, A. (2018). Control empresarial del uso de medios tecnológicos, ¿caso cerrado? *Revista de Información Laboral*.

Agencia Española de Protección de datos. (2010). *Informe jurídico 0201/2010.* Gabinete jurídico. Obtenido de https://www.aepd.es/es/documento/2010-0201.pdf

Agencia Española de Protección de Datos. (13 de Marzo de 2020). *aepd.* Obtenido de FAQ sobre el COVID-19: https://www.aepd.es/es/node/44455

Aranzadi Instituciones. (s.f.). Obtenido de Derechos y deberes: La protección de datos de carácter personal en la relación de trabajo: https://insignis-aranzadidigital-es.unileon.idm.oclc.org/maf/app/document?srguid=i0ad82d9b0000017231ecdfe25ef0cc58&marginal=DOC\2003\89&docguid=I1dfa4da0759d11db9c4701000000000&ds=ARZ_LEGIS_CS&infotype=arz_doctrina;&spos=1&epos=1&td=8&predefinedRelations

Bonilla Blasco, J. (2001). Los efectos jurídicos del correo electrónico en el ámbito laboral. *Relaciones Laborales: Revista crítica de teoría y práctica*(2), 1177-1188.

Cabeza Pereiro, J. (2018). El necesario cambio en la jurisprudencia constitucional sobre video vigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH. *Temas laborales: Revista andaluza de trabajo y bienestar social*(141), 13-36.

Cardona Rubert, M. B. (2003). Las relaciones laborales y el uso de las tecnologías informáticas. *Lan harremanak: Revista de relaciones laborales*(1), 157-173.

Catoira, A. A. (2011). Los derechos de la generación electrónica en el ámbito laboral. *Revista de Derecho, 12*(1), 257-281.

Desdentando Bonete, A., & Desdentado Daroca, E. (2018). La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el contol del uso laboral del ordenador. *Revista de Información Laboral*(1).

Fernández Orrico, F. J. (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.

García Murcia, J., & Rodríguez Cardo, I. A. (2019). La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo. *Nueva revista española de derecho del trabajo*(216), 19-64.

García-Perrote Escartín, I., & Mercader Uguina, J. (2018). El protagonismo del convenio colectivo en el nuevo reglamento de protección de datos. *Revista de Información Laboral*.

Muñiz Aguirreurreta, D. (2020). COVID-19. Relaciones laborales y protección de datos. *Aranzadi digital*(1).

Navarro Nieto, F. (2012). Los reconocimientos médicos como instrumento de vigilancia de la salud laboral: condicionantes legales y jurisprudenciales. *Aranzadi Social: Revista Doctrinal, 4*(11), 151-166.

Ortega Giménez, A. (2019). Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de datos de la UE. *Nueva revista española de derecho del trabajo*(216), 133-180.

Poquet Catalá, R. (2016). De nuevo con las listas negras. *Revista de Información Laboral*(12), 59-70.

Quílez Moreno, J. (2019). La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores. *Nueva revista española de derecho del trabajo*(217), 127-152.

Ribas, X. (2020). Control de la temperatura del trabajador: opinión sobre el comunicado de la AEPD. *Aranzadi digital*(1).

Rodriguez Escanciano, S. (2015). *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores.* Valencia: Tirant Lo Blanch.

Rojas Rosco, R., & López Carballo, D. (2018). El impacto del RGPD en el ámbito del control laboral y la era de la innovación. *Actualidad Civil*(5), 8.

Tacón López, R. (2005). El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado en cuestión. *Civitas, Navarra*, 103.

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.

Toscani Giménez, D., & Calvo Morales, D. (2014). El uso de internet y el correo electrónico en la empresa: límites y garantías. *Revista Española de Derecho del Trabajo*(165), 197-224.

Zaragoza Tejada, J. I. (2020). La prueba obtenida por videocámaras de seguridad tras la STEDH del 17 de octubre del 2019. Caso López Ribalda vs España. *Revista Aranzadi Doctrinal*(2), 8.